GFI Product Manual

GFI EventsManager™

Administrator Guide

GFI®

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

All product and company names herein may be trademarks of their respective owners.

GFI EventsManager is copyright of GFI SOFTWARE Ltd. - 1999-2013 GFI Software Ltd. All rights reserved.

Document Version: 13.0.0

Last updated (month/day/year): 1/30/2013

Contents

1 Introduction **21**

1.1 About GFI EventsManager 21
1.2 How GFI EventsManager works 23
1.2.1 Stage 1: Event Collection 24
1.2.2 Stage 2: Event Processing 24
1.3 Conventions used in this guide 25

2 Installing GFI EventsManager **26**

2.1 Deployment scenarios 26
2.1.1 Installing GFI EventsManager in a Local Area Network (LAN) 28
2.1.2 GFI EventsManager within a Demilitarized Zone (DMZ) 29
2.1.3 GFI EventsManager within a Wide Area Network (WAN) 31
2.2 System requirements 32
2.2.1 Hardware requirements 32
2.2.2 Supported operating systems (32-bit and 64-bit) 32
2.2.3 Other software components 33
2.2.4 Storage requirements 33
2.2.5 Firewall ports and protocols 33
2.2.6 Firewall permissions 34
2.2.7 Event source settings 34
2.2.8 Antivirus exceptions 35
2.2.9 Computer identification considerations 35
2.2.10 Collecting event logs from computers running Microsoft® Vista or later 35
2.3 Upgrading GFI EventsManager 35
2.3.1 Upgrading from a previous version 36
2.4 Installing a new instance of GFI EventsManager 44
2.4.1 Installation procedure 44
2.5 Testing the installation 53
2.5.1 Process events - Local computer 54
2.5.2 Process events - Local domain 56
2.5.3 Process events - Selected machines 59

3 Achieving Results **62**

3.1 Achieving Network Security 62
3.2 Effective System Health Monitoring 64
3.3 Achieving PCI DSS Compliance 66

4 Managing Event Sources **67**

4.1 Adding event sources manually 67
4.2 Adding event sources automatically 68
4.3 Creating a new event source group 71
4.4 Configuring event source properties 73
4.4.1 Configuring general event source properties 73
4.4.2 Configuring event source logon credentials 74
4.4.3 Configuring event source license type 76

4.4.4 Configuring event source operational time 77
4.4.5 Configuring event source monitoring 78
4.4.6 Configuring event processing parameters 80
4.5 Database sources 81
4.5.1 Microsoft® SQL Server® Sources 81
4.5.2 Oracle server sources 89

5 Collecting Event Logs 100

5.1 Collecting Windows® event logs 100
5.2 Collecting Text logs 103
5.3 Collecting Syslogs 106
5.3.1 Configuring the Syslog server communications port 109
5.4 Collecting SNMP Traps Messages 110
5.4.1 Configuring the SNMP Trap server 113
5.5 Collecting custom logs 114
5.6 Collecting GFI LanGuard event logs 116
5.6.1 How to enable GFI LanGuard event logging? 117
5.7 Collecting GFI EndPointSecurity events 121

6 Browsing Stored Events 123

6.1 Navigating the Events Browser 123
6.2 Using the Events Browser 124
6.2.1 Exporting events to CSV 124
6.2.2 Creating reports from views 125
6.2.3 Deleting events 126
6.2.4 Searching stored events 127
6.2.5 Identifying rules using the rule finder tool 127
6.3 Managing Events Browser views 127
6.3.1 Creating Root Views and Views 127
6.3.2 Editing a view 130
6.3.3 Deleting a view 130
6.4 Customizing Events Browser layout 130
6.4.1 Customizing description position 130
6.4.2 Event color-coding options 131
6.5 Browsing events from different databases 132

7 Activity Monitoring 134

7.1 General Status view 134
7.2 Job Activity view 138
7.3 Statistics view 139

8 Reporting 141

8.1 Navigating the Reports tab 142
8.2 Available reports 143
8.3 Managing reports 144
8.3.1 Creating a root folder 144
8.3.2 Creating a folder 146

8.4 Creating a root report 146
8.5 Creating custom reports 151
8.6 Generating reports 158
8.6.1 Generating a report 158
8.6.2 Generating daily digest reports 159
8.6.3 Generating settings reports 161
8.6.4 Generating rules reports 163
8.6.5 Generating operational history reports 164
8.6.6 Generating activity overview reports 166
8.7 Analyzing reports 168
8.8 Defining column headings 169
8.8.1 Reporting on events from different databases 170
8.9 Customizing HTML reports 170

9 Events Processing Rules 173

9.1 About events processing rules 173
9.1.1 Event classification 174
9.2 Managing rules-set folders 175
9.2.1 Available rule-sets 175
9.2.2 Adding a rule-set folder 177
9.2.3 Renaming and Deleting a rule-set folder 177
9.3 Creating new events processing rules 178
9.4 Creating new rules from existing events 183
9.5 Advanced event filtering parameters 188
9.5.1 Windows® event filtering parameters 188
9.5.2 Syslog filtering parameters 188
9.6 Prioritizing events processing rules 189

10 Active Monitoring 190

10.1 About Active Monitoring Checks 190
10.2 Creating and configuring a root folder 192
10.3 Adding sub-folders to a root folder 196
10.4 Creating and configuring active monitoring checks 201
10.5 Applying active monitoring checks 206
10.6 Deleting folders and monitoring checks 207

11 Alerts and Default Actions 208

11.1 Configuring Default Classification Actions 208
11.2 Configuring Alerting Options 210
11.2.1 Email alerts 212
11.2.2 Network alerts 213
11.2.3 SMS alerts 214
11.2.4 SNMP alerts 215
11.2.5 General settings 215

12 User Groups 216

12.1 Configuring the administrator account 216

12.2 Managing user accounts 222
12.2.1 Creating a new user account 222
12.2.2 Changing user account properties 228
12.2.3 Deleting a user account 229
12.3 Managing user groups 229
12.3.1 Creating a new group 229
12.3.2 Changing group properties 231
12.3.3 Deleting a group 231

13 Console Security and Audit Options 232

13.1 Enabling login system 232
13.1.1 Password recovery 234
13.2 Anonymization 235
13.3 Auditing console activity 238
13.4 Auto-discovery credentials 239

14 Database Maintenance 242

14.1 Managing the database backend 242
14.1.1 Creating a new database 242
14.1.2 Protecting your database 243
14.1.3 Database record hashing 245
14.1.4 Switching between file storage databases 247
14.1.5 Configuring database rotation options 250
14.1.6 Configuring Database Operations 251
14.2 Creating maintenance jobs 252
14.2.1 Import from file 253
14.2.2 Export to file 257
14.2.3 Export to SQL 261
14.2.4 Copy data 266
14.2.5 Commit deletions 269
14.2.6 Import from SQL Server® Database 271
14.2.7 Import from legacy files 275
14.2.8 Import from legacy file storage 279
14.3 Editing maintenance jobs 281
14.3.1 Viewing scheduled maintenance jobs 281
14.3.2 Editing maintenance job properties 282
14.3.3 Changing maintenance jobs priority 284
14.3.4 Deleting a maintenance job 284

15 Configuring the Management Console 285

15.1 Performance options 285
15.2 Product updates 286
15.2.1 Downloading updates directly 287
15.2.2 Downloading updates from an alternate location (offline) 288
15.3 Product licensing 293
15.3.1 Updating license key 293
15.3.2 Obtaining a free 30-day trial license key 294

15.3.3 Viewing license details 294
15.3.4 Purchasing a license key 294
15.4 Product version information 294
15.4.1 Checking your GFI EventsManager version 294
15.4.2 Checking for newer versions 295
15.5 Importing and Exporting settings 295
15.5.1 Exporting configurations to a file 296
15.5.2 Importing configurations from a file 298
15.5.3 Importing configurations from another instance 300
15.6 Building query restrictions 302
15.6.1 Using the Edit Query Restriction dialog 303

16 Command Line Tools 307

16.1 Using ESMCmdConfig.exe 307
16.1.1 /op:registerService 308
16.1.2 /op:enable 308
16.1.3 /op:disable 308
16.1.4 /op:SetLicense 308
16.1.5 /op:configureAlerting 309
16.1.6 /op:setAdminEmail 309
16.1.7 /op:createProgramGroupShortcuts 309
16.1.8 /op:removeProgramGroupShortcuts 310
16.1.9 /op:getComputers 310
16.2 Using EsmDlibM.exe 310
16.2.1 /importFromSQL 311
16.2.2 /importFromDlib 311
16.2.3 /copyData 312
16.2.4 /importFromLegacyFile 314
16.2.5 /exportToFile 314
16.2.6 /importFromFile 316
16.2.7 /commitDeletedRecords 317
16.2.8 /exoportToSQL 317
16.3 Using DLibAdm.exe 318
16.3.1 /decryptDatabase 319
16.3.2 /encryptDatabase 319
16.3.3 /displayAllDLib 319
16.3.4 /copyMoveDLib 320
16.4 Using EsmReport.exe 320
16.4.1 Generate Configuration reports 321
16.4.2 Generate Status reports 321
16.4.3 Generate Events reports 322
16.4.4 Using ImportSettings.exe 323
16.4.5 Using ExportSettings.exe 324

17 Miscellaneous 326

17.1 Enabling event source permissions manually 326
17.1.1 Enabling permissions on Microsoft® Windows® XP 326

17.1.2 Enabling permissions on Microsoft® Windows® Vista 327
17.1.3 Enabling permissions on Microsoft® Windows® 7 330
17.1.4 Enabling permissions on Microsoft® Windows® Server 2003 332
17.1.5 Enabling permissions on Microsoft® Windows® Server 2008 (including R2) 333
17.2 Enabling event source permissions automatically 334
17.2.1 Enabling permissions on Windows® Server 2003 via GPO 334
17.2.2 Enabling permissions on Windows® Server 2008 via GPO 335
17.3 Disabling User Account Control (UAC) 339

18 Troubleshooting **340**

18.1 Documentation 340
18.2 GFI SkyNet 340
18.3 Request technical support 340
18.4 Web forum 340
18.5 Troubleshooter wizard 340

19 Glossary **347**

20 Index **351**

List of Figures

Screenshot 1: GFI EventsManagerintegrates into any existing IT infrastructure 21
Screenshot 2: The GFI EventsManager operational stages 23
Screenshot 3: Export data from remote sites to the main instance of GFI EventsManager 31
Screenshot 4: Upgrade prerequisite check 36
Screenshot 5: DLib Database Server 37
Screenshot 6: DLib Database Server EULA 37
Screenshot 7: DLib install folder 38
Screenshot 8: Start installing DLib Database Server 38
Screenshot 9: Delete old version files 39
Screenshot 10: GFI EventsManager setup wizard welcome screen 39
Screenshot 11: GFI EventsManager EULA 40
Screenshot 12: GFI EventsManager registration details 40
Screenshot 13: Remote logon credentials for event log monitoring 41
Screenshot 14: GFI EventsManager install folder 42
Screenshot 15: GFI EventsManager installation completed 42
Screenshot 16: Auto updates check 43
Screenshot 17: Set the database backend 43
Screenshot 18: Upgrade prerequisite check 45
Screenshot 19: DLib Database Server 46
Screenshot 20: DLib Database Server EULA 46
Screenshot 21: DLib install folder 47
Screenshot 22: Start installing DLib Database Server 47
Screenshot 23: GFI EventsManager setup wizard welcome screen 48
Screenshot 24: GFI EventsManager EULA 49
Screenshot 25: GFI EventsManager registration details 49
Screenshot 26: Remote logon credentials for event log monitoring 50
Screenshot 27: GFI EventsManager install folder 51
Screenshot 28: GFI EventsManager installation completed 51
Screenshot 29: Auto updates check 52
Screenshot 30: Set the database backend 52
Screenshot 31: Running GFI EventsManager for the first time 53
Screenshot 32: Process events - Local computer 54
Screenshot 33: Console main actions 55
Screenshot 34: Process events - Local domain 56
Screenshot 35: Automatic discovery wizard 57
Screenshot 36: Select event source types to detect on your network 57
Screenshot 37: Search network progress 58
Screenshot 38: Process events - Selected machines 59

Screenshot 39: Add new event source wizard 60
Screenshot 40: Add new event source wizard 67
Screenshot 41: Synchronization properties - General tab 69
Screenshot 42: Excluding computers from automatic synchronization 70
Screenshot 43: Synchronization properties -Schedule tab 71
Screenshot 44: Add new event source group 72
Screenshot 45: Event sources properties dialog 74
Screenshot 46: Configuring alternative logon credentials 75
Screenshot 47: Configuring event source license type 77
Screenshot 48: Specify operational time 78
Screenshot 49: Event source properties - Monitoring tab 79
Screenshot 50: Event processing configuration tabs 80
Screenshot 51: Database Servers Groups 81
Screenshot 52: Configure logon settings from the Logon Credentials tab 82
Screenshot 53: Configure the normal working hours from Operational Time tab 83
Screenshot 54: Configure SQL Server Auditing from SQL Server Audit tab 84
Screenshot 55: Add new Microsoft® SQL server 86
Screenshot 56: Microsoft® SQL Database properties: General tab 87
Screenshot 57: Microsoft® SQL Database properties: Connection Settings tab 88
Screenshot 58: Microsoft® SQL Database properties: Settings tab 89
Screenshot 59: Database Servers Groups 90
Screenshot 60: Oracle Database group - General tab 91
Screenshot 61: Oracle Database group - Logon Credentials tab 92
Screenshot 62: Oracle Database group - Operational Time tab 93
Screenshot 63: Oracle Database group - Oracle Audit tab 94
Screenshot 64: Add new Oracle server 95
Screenshot 65: Oracle Server properties - General tab 96
Screenshot 66: Oracle Server properties - Connection Settings tab 97
Screenshot 67: Oracle Server properties - Audit by Objects tab 98
Screenshot 68: Oracle Server properties - Audit by Statements tab 99
Screenshot 69: Computer group properties: Configuring Windows® Event Logs parameters 101
Screenshot 70: Selecting event logs to collect 102
Screenshot 71: Configuring Windows Event Log Processing parameters 103
Screenshot 72: Text logs options 104
Screenshot 73: Adding folders containing Text Logs 105
Screenshot 74: Syslog messages must be directed to the computer running GFI EventsManager 107
Screenshot 75: Collecting Syslogs - Syslogs options 108
Screenshot 76: Configuring Syslog Server communication port 109
Screenshot 77: Syslog server options 110
Screenshot 78: SNMP Trap messages must be directed to the computer running GFI EventsManager 111

Screenshot 79: Collecting SNMP Traps 112
Screenshot 80: Configuring SNMP Traps 113
Screenshot 81: SNMP Traps options 114
Screenshot 82: Custom event logs setup 115
Screenshot 83: Custom event logs dialog 116
Screenshot 84: Enabling GFI LanGuard logging through the registry 118
Screenshot 85: Add Windows® Application logs 119
Screenshot 86: Add GFI LanGuard rules 120
Screenshot 87: Events Browser 123
Screenshot 88: Export events tool 125
Screenshot 89: Report from view button 125
Screenshot 90: Event finder tool 127
Screenshot 91: Custom view builder 128
Screenshot 92: Edit view restriction 129
Screenshot 93: Customize View tab 129
Screenshot 94: Sample: New Root Views and Views 130
Screenshot 95: Customize browser description 130
Screenshot 96: Color coding configuration 131
Screenshot 97: Advanced Color Filter 132
Screenshot 98: Switch database dialog 133
Screenshot 99: GFI EventsManager Status: General view 135
Screenshot 100: GFI EventsManager Status: Job Activity view 138
Screenshot 101: GFI EventsManager Status: Statistics view 140
Screenshot 102: Navigating the Reporting UI 142
Screenshot 103: Create Report Folder dialog 145
Screenshot 104: Creating a root report 146
Screenshot 105: Configuring new root report layout options 147
Screenshot 106: Inserting a chart in a new root report 148
Screenshot 107: Configuring the schedule for when the report is generated 149
Screenshot 108: Create new report Options 150
Screenshot 109: Record limit settings 151
Screenshot 110: Creating a root report 152
Screenshot 111: Configuring new root report layout options 153
Screenshot 112: Inserting a chart in a new root report 154
Screenshot 113: Configuring the schedule for when the report is generated 155
Screenshot 114: Create new report Options 156
Screenshot 115: Record limit settings 157
Screenshot 116: Generating a report 158
Screenshot 117: Report sample 159
Screenshot 118: Daily Digest email settings 160

Screenshot 119: Daily digest email 161
Screenshot 120: Generate configuration report 162
Screenshot 121: Settings report sample 163
Screenshot 122: Generate configuration report 164
Screenshot 123: Operational History report 165
Screenshot 124: Operational History dialog 165
Screenshot 125: Operational History report sample 166
Screenshot 126: Activity overview : Export button 166
Screenshot 127: Activity overview dialog 167
Screenshot 128: Activity overview report sample 167
Screenshot 129: Analyzing reports 168
Screenshot 130: Define custom column conditions 169
Screenshot 131: Switch database dialog 170
Screenshot 132: Editing HTML report templates 171
Screenshot 133: How Events Processing Rules work 174
Screenshot 134: Rule-sets folder and Rule-sets 175
Screenshot 135: Creating a new rule 178
Screenshot 136: Select the logs which the rule will be applied to 179
Screenshot 137: Configure the rule conditions 180
Screenshot 138: Select event occurrence and importance 181
Screenshot 139: Select the triggered action 182
Screenshot 140: Creating a rule from an existing event 184
Screenshot 141: New rule from event - General settings 185
Screenshot 142: New rule from event - Select logs to collect 186
Screenshot 143: New rule from event - Add conditions 187
Screenshot 144: How Active Monitoring Checks work 191
Screenshot 145: Root folder and sub-folder structure 192
Screenshot 146: Folder properties - General tab 193
Screenshot 147: Folder properties - Target computer tab 193
Screenshot 148: Folder properties - Schedule tab 194
Screenshot 149: Folder properties - Action events tab 195
Screenshot 150: Folder properties - General tab 196
Screenshot 151: Folder properties - Target computer tab 197
Screenshot 152: Folder properties - Schedule tab 198
Screenshot 153: Folder properties - Action events tab 199
Screenshot 154: Creating a new active monitoring check 201
Screenshot 155: Select check type 202
Screenshot 156: Configure general check properties 202
Screenshot 157: Configure monitoring check parameters 203
Screenshot 158: Select the effected sources 203

Screenshot 159: Set the scan time interval 204
Screenshot 160: Configure event log actions 205
Screenshot 161: Target computers tab 206
Screenshot 162: Deleting folders and monitoring checks 207
Screenshot 163: Configuring default classification actions 208
Screenshot 164: Default Classification Actions dialog 209
Screenshot 165: Configuring Alerting Options 211
Screenshot 166: Configuring Email options 212
Screenshot 167: Configuring Network options 213
Screenshot 168: Configuring Network alerts: Format message 213
Screenshot 169: Configuring SMS options 214
Screenshot 170: Configuring SNMP alerts 215
Screenshot 171: Configuring EventsManagerAdministrator account 217
Screenshot 172: EventsManagerAdministrator properties 217
Screenshot 173: Configuring user typical working hours 218
Screenshot 174: Configure alerts outside working hours 219
Screenshot 175: Select the group which the user account is a member of 220
Screenshot 176: Configuring user account privileges 221
Screenshot 177: User account filtering 222
Screenshot 178: Creating a new user 223
Screenshot 179: Creating a new user - General properties 223
Screenshot 180: Creating a new user - Working hours 224
Screenshot 181: Creating a new user - Alerting options 225
Screenshot 182: Creating a new user - Select notification group(s) 226
Screenshot 183: Creating a new user - Privileges 227
Screenshot 184: User filtering options 228
Screenshot 185: Creating a new user group 229
Screenshot 186: Creating a new user group - General properties 230
Screenshot 187: Creating a new user group - General properties 231
Screenshot 188: Editing console security options 233
Screenshot 189: Enabling EventsManager login system 234
Screenshot 190: Login credentials prompt 235
Screenshot 191: Enable console anonymization 236
Screenshot 192: Anonymization options 237
Screenshot 193: Enabling console user activity auditing 238
Screenshot 194: Audit Options dialog 239
Screenshot 195: Configuring Auto-Discovery Credentials 240
Screenshot 196: Specify Auto-discovery credentials 241
Screenshot 197: File storage system dialog 243
Screenshot 198: Editing file storage settings 244

Screenshot 199: Enabling encryption 245
Screenshot 200: Enabling / disabling record hashing 246
Screenshot 201: Record hashing dialog 247
Screenshot 202: Options tab 248
Screenshot 203: Switch between databases from the dashboard 249
Screenshot 204: Configuring database rotation options 250
Screenshot 205: Database Operations Options dialog 252
Screenshot 206: Creating Import\Export jobs 254
Screenshot 207: Import from file 254
Screenshot 208: Import from file - Specify import file path 255
Screenshot 209: Decrypt secure import files 255
Screenshot 210: Add filtering conditions 256
Screenshot 211: Execute job options 257
Screenshot 212: Creating Import\Export jobs 258
Screenshot 213: Export to file 258
Screenshot 214: 259
Screenshot 215: Decrypt/Encrypt data 259
Screenshot 216: Filtering export data 260
Screenshot 217: Execute job options 261
Screenshot 218: Creating Import\Export jobs 262
Screenshot 219: Export to SQL 262
Screenshot 220: Specifying SQL Server details 263
Screenshot 221: Select columns to export 264
Screenshot 222: Filtering export data 265
Screenshot 223: Execute job options 266
Screenshot 224: Creating Import\Export jobs 267
Screenshot 225: Select Copy data job 267
Screenshot 226: Specify source and destination databases 268
Screenshot 227: Decrypt source and encrypt destination databases 268
Screenshot 228: Filtering export data 269
Screenshot 229: Creating Import\Export jobs 270
Screenshot 230: Create commit deletion jobs 270
Screenshot 231: Select database to delete records from 271
Screenshot 232: Creating Import\Export jobs 272
Screenshot 233: Select Import from SQL Server Database 272
Screenshot 234: Specify SQL Server address and login details 273
Screenshot 235: Decrypt anonymized databases 274
Screenshot 236: Add filtering conditions to filter unwanted data 274
Screenshot 237: Specify when the maintenance job is executed 275
Screenshot 238: Creating Import\Export jobs 276

Screenshot 239: Import from legacy files 276
Screenshot 240: Specify import file location 277
Screenshot 241: Decrypt the information in the import file 277
Screenshot 242: Remove anonymization 278
Screenshot 243: Filter unwanted events through filtering conditions 278
Screenshot 244: Specify when the maintenance job is executed 279
Screenshot 245: Creating Import\Export jobs 280
Screenshot 246: Import legacy file storage data 280
Screenshot 247: Specify when the maintenance job is executed 281
Screenshot 248: Maintenance job activity 282
Screenshot 249: Viewing scheduled maintenance jobs 282
Screenshot 250: Maintenance job properties dialog 283
Screenshot 251: Maintenance job priorities 284
Screenshot 252: GFI EventsManager Performance Options 285
Screenshot 253: Performance Options dialog 286
Screenshot 254: Configure auto update options 287
Screenshot 255: Configuring proxy settings to download product updates 288
Screenshot 256: GFI EventsManager updates 289
Screenshot 257: GFI EventsManager updates repository 290
Screenshot 258: Open CMD in administrator mode 291
Screenshot 259: Change path to GFI EventsManager install directory 292
Screenshot 260: Manually launch an update session 292
Screenshot 261: Updates status 293
Screenshot 262: Update license key dialog 293
Screenshot 263: Buy now! Button 294
Screenshot 264: Version Information screen 295
Screenshot 265: Export configurations to a file 296
Screenshot 266: Specify export destination 297
Screenshot 267: Select export configurations 297
Screenshot 268: Import configurations from a file 298
Screenshot 269: Specify configuration file location 299
Screenshot 270: Select configurations to import 299
Screenshot 271: Import configurations from another instance of GFI EventsManager 300
Screenshot 272: Specify instance location 301
Screenshot 273: Select configurations to import from another instance of GFI EventsManager 301
Screenshot 274: Users, Events processing rules and Report queries 303
Screenshot 275: Defining restrictions: Editing a query restriction 304
Screenshot 276: Defining restrictions: Customizing the condition 305
Screenshot 277: Firewall rules on Microsoft® Windows® XP 327
Screenshot 278: Local security policy window 328

Screenshot 279: Audit object access properties 329
Screenshot 280: Allowed programs in Microsoft® Windows® Vista or later 330
Screenshot 281: Local security policy window 331
Screenshot 282: Audit object access Properties 332
Screenshot 283: Enable firewall rules in Microsoft® Windows® Server 2003 333
Screenshot 284: Firewall rules on Microsoft® Windows® Server 2008 334
Screenshot 285: Domain Policy console in Microsoft® Windows® Server 2003 335
Screenshot 286: Group Policy Management in Microsoft® Windows® Server 2008 R2 336
Screenshot 287: Group Policy Management Editor 337
Screenshot 288: Predefined rules 338
Screenshot 289: Disabling UAC 339
Screenshot 290: Select information gathering mode 341
Screenshot 291: Troubleshooter automatic checks 342
Screenshot 292: Troubleshooter automatically fixing detected issues 342
Screenshot 293: If the problem persists, search for articles on our knowledge base 343
Screenshot 294: Manually checking for issues 343
Screenshot 295: Specify contact details 344
Screenshot 296: Key in the problem description and other information 344
Screenshot 297: Gathering machine information 345
Screenshot 298: Finalizing the troubleshooting process 345

List of Tables

Table 1: GFI EventsManager engines 24
Table 2: Terms and conventions used in this manual 25
Table 3: Devices supported by GFI EventsManager 28
Table 4: Benefits of installing GFI EventsManager in DMZ 30
Table 5: Hardware requirements 32
Table 6: Storage space requirements 33
Table 7: Firewall ports and protocols 33
Table 8: Firewall permissions 34
Table 9: Event source settings 34
Table 10: Upgrading GFI EventsManager 36
Table 11: Components installed using EventsManager.exe 44
Table 12: Quick Launch Console options 53
Table 13: Quick Launch Console options 55
Table 14: Adding new event sources manually 60
Table 15: Adding new event sources manually 68
Table 16: Synchronization properties - General tab 69
Table 17: Event source group options 72
Table 18: Event source properties - General options 74
Table 19: License types 76
Table 20: Event source monitoring options 79
Table 21: Microsoft® SQL Database group: General tab 81
Table 22: Microsoft® SQL Database group: Logon Credentials 82
Table 23: Microsoft® SQL Database group -SQL Server® Audit 84
Table 24: Microsoft® SQL Database group - Settings 85
Table 25: Microsoft® SQL Database - General tab options 87
Table 26: Microsoft® SQL Database - Connection Settings tab 88
Table 27: Microsoft® SQL Database - Settings tab options 89
Table 28: Oracle Server supported audits 89
Table 29: Oracle Server configuration stages 90
Table 30: Oracle Database group - General tab 91
Table 31: Oracle Database group - Oracle Audit 94
Table 32: Oracle Server properties - General tab 96
Table 33: Oracle Server properties - Connection Settings tab 97
Table 34: Oracle Server properties - Audit by Objects tab 98
Table 35: Oracle Server properties - Audit by Statements tab 99
Table 36: Windows® Event Logs collected by GFI EventsManager 100
Table 37: Information gathered by GFI LanGuard 116
Table 38: GFI EndPointSecurity supported devices 121

Table 39: Navigating the Events Browser 124
Table 40: Event Browser: Create new report 126
Table 41: Event Browser: Create new view 128
Table 42: Description pane positions 131
Table 43: Status monitoring: General view sections 135
Table 44: Status monitoring: Job activity view 139
Table 45: Status monitoring: Statistics view 140
Table 46: Navigating the Reporting tab 142
Table 47: Available reports 143
Table 48: Create report folder: Schedule options 145
Table 49: Range pattern options 150
Table 50: Report record settings 151
Table 51: Range pattern options 156
Table 52: Report record settings 157
Table 53: Daily digest email description 161
Table 54: Settings report heading information 161
Table 55: Rules report heading information 163
Table 56: Operational History report description 164
Table 57: Operational History export options 165
Table 58: Activity overview report headings 166
Table 59: Export Operational History options 167
Table 60: Analyzing reports: Tools 168
Table 61: Add Column Definition options 169
Table 62: Default HTML templates 171
Table 63: HTML template: Editable sections 172
Table 64: HTML report template placeholders 172
Table 65: Common available rule-set folders 176
Table 66: Configuring new events processing rules: Actions 182
Table 67: Available event processing rule actions 187
Table 68: Windows® event filtering parameters: Event ID field 188
Table 69: Windows® event filtering parameters: Source, Category and User fields 188
Table 70: Syslog filtering parameters: Message and Process fields 188
Table 71: Monitoring checks - Action events 195
Table 72: Monitoring checks - Action events 200
Table 73: Monitoring checks - Action events 205
Table 74: Default Classification Actions 209
Table 75: Alerting Options dialog - Email alerts 212
Table 76: Alerting Options dialog: SMS 214
Table 77: Alerting Options: SNMP Traps 215
Table 78: Alerting Options: General settings 215

Table 79: User filtering options 228
Table 80: Database rotation options 251
Table 81: Configuring database operations 252
Table 82: Maintenance jobs types 253
Table 83: Creating maintenance jobs - Schedule options 257
Table 84: Filtering export data 260
Table 85: Creating maintenance jobs - Schedule options 261
Table 86: Database operations: Export file name structure 261
Table 87: Export to SQL - Server options 263
Table 88: Filtering export data 265
Table 89: Creating maintenance jobs - Schedule options 266
Table 90: Filtering export data 269
Table 91: Creating maintenance jobs - Schedule options 269
Table 92: Creating maintenance jobs - Schedule options 271
Table 93: Export to SQL - Server options 273
Table 94: Auto update options 287
Table 95: Uses of query restrictions 302
Table 96: Launching the Edit Query Restrictions dialog 303
Table 97: Defining restrictions: Field Operators 304
Table 98: Defining restrictions: Query Condition tools 305
Table 99: /op:registerService Parameters 308
Table 100: /op:disable Parameter 308
Table 101: /op:SetLicense Parameters 308
Table 102: /op:configureAlerting Parameters 309
Table 103: /op:setAdminEmail Parameter 309
Table 104: /op:getComputers Parameter 310
Table 105: /importFromSQL Parameters 311
Table 106: /importFromDlib Parameters 311
Table 107: /copyData Parameters 312
Table 108: /importFromLegacyFile Parameters 314
Table 109: /exportToFile 314
Table 110: /importFromFile Parameters 316
Table 111: /commitDeletedRecords Parameters 317
Table 112: /exportToSQL Parameters 317
Table 113: /decryptDatabase Parameters 319
Table 114: /encryptDatabase Parameters 319
Table 115: /displayAllDLib Parameters 320
Table 116: /copyMoveDLib 320
Table 117: Configurations report parameters 321
Table 118: Status report parameters 322

Table 119: Events reports parameters 322
Table 120: CMD: ImportSettings.exe parameters 323
Table 121: CMD: ExportSettings.exe parameters 324

1 Introduction

The enormous volume of system event logs generated daily is of growing importance to organizations that must record information for forensic and compliance purposes. It is essential to perform real-time network-wide event log monitoring, analysis and reporting to address any incidents or security concerns and combat threats to business continuity.

GFI EventsManager assists with this monumental task by automatically and centrally monitoring and managing event logs - supporting a wide range of event types generated both by applications and devices from top vendors as well as for custom ones.

This chapter provides you with information about how events management is achieved using GFI EventsManager.

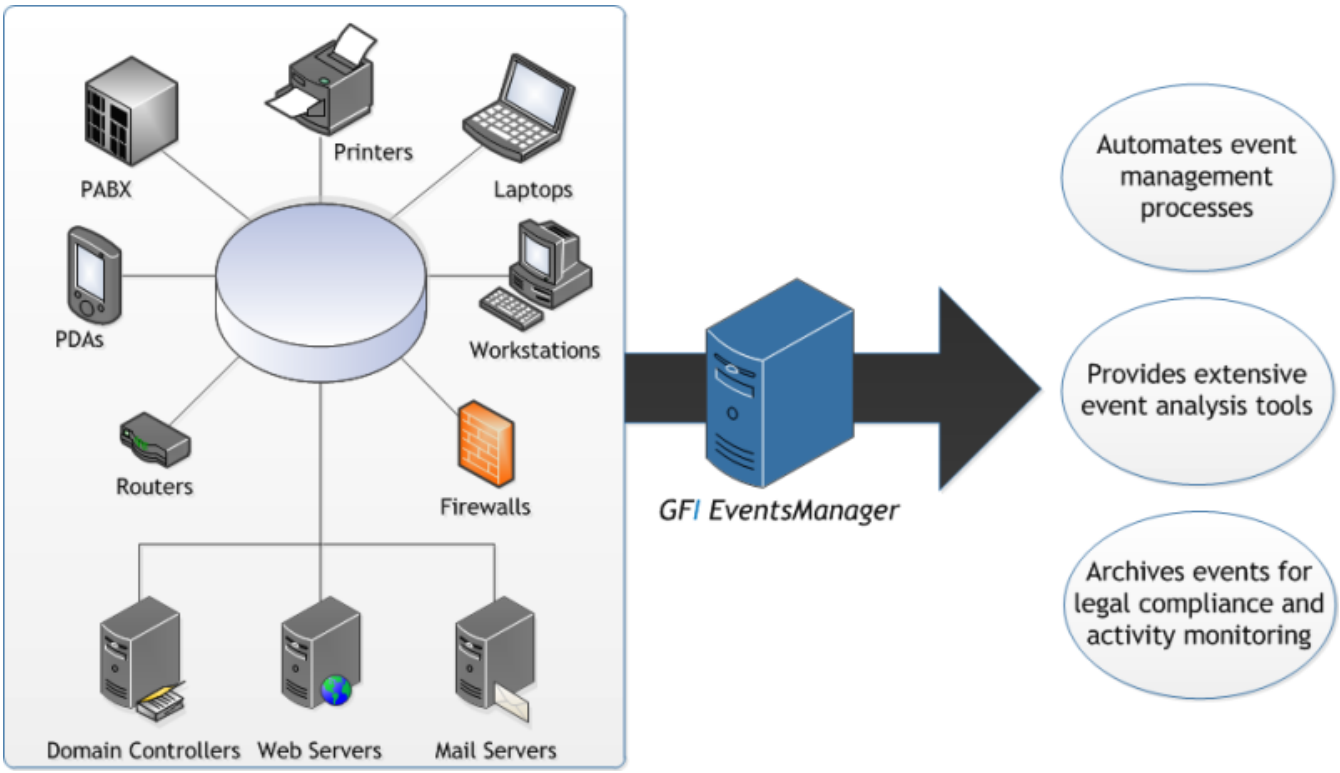
Topics in this chapter:

1.1 About GFI EventsManager 21

1.2 How GFI EventsManager works 23

1.3 Conventions used in this guide 25

1.1 About GFI EventsManager



Screenshot 1: GFI EventsManagerintegrates into any existing IT infrastructure

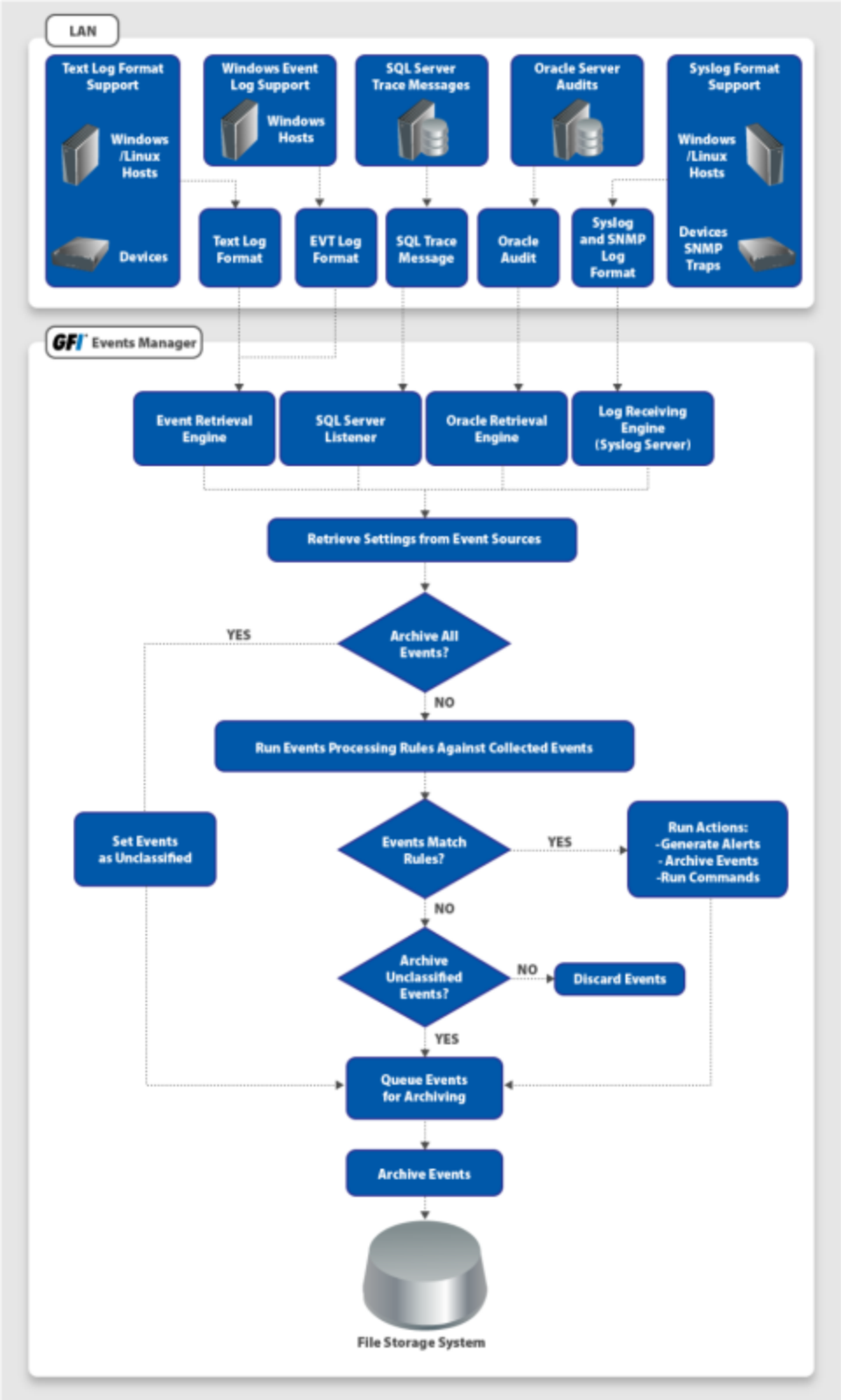
GFI EventsManager is a results oriented event log management solution which integrates into any existing IT infrastructure, automating and simplifying the tasks involved in network-wide events management.

Through the features supported by GFI EventsManager, you are able to:

- Automatically monitor computers and network devices through GFI EventsManager's wide range of event log support; such as Text Logs, Windows® Event Logs, Syslogs, SNMP Traps Messages, Active Monitoring Events and even custom event logs
- Monitor computers and services running on your network through active monitoring features such as continuous checking of HTTP/HTTPS/FTP site availability, server roles queries, firewall queries and more
- Optimize security and performance while tracking operational issues by auditing your critical systems/devices; such as routers, firewall, sensors, servers and database engines
- Create and maintain an automated network security system which detects intrusion attacks
- Achieve compliance with various regulations and acts including SOX, PCI DSS, Code of Connection, HIPAA, data protection laws and others
- Proactively detect events which will lead to disaster such as hardware failure. When such events are processed, GFI EventsManager provides an early warning to give you control and take corrective action
- Minimize the risk and business loss due to systems downtime and misconfiguration
- Easily browse events from any number of databases through the extensive Events Browser; which helps you carry out forensic investigations with minimal human input
- Automatically processes and archives event logs, collecting and highlighting the information you need to know about the most important events occurring in your network so you are never caught off guard
- Generate technical IT level and management level reports from the extensive list of reports and also create new ones from existing reports or collected events
- Protect your business by tracking the security events in your network. Find who is responsible for security breaches and network threats

For a full list of features, refer to: http://www.gfi.com/eventsmanager#features

1.2 How GFI EventsManager works



Screenshot 2: The GFI EventsManager operational stages

The operational functionality of GFI EventsManager is divided in the following stages:

- Stage 1: Event Collection
- Stage 2: Event Processing

1.2.1 Stage 1: Event Collection

During the Event Collection stage, GFI EventsManager collects logs from specific event sources. This is achieved through the use of two event collection engines: The **Event Retrieval Engine** and the **Event Receiving Engine**.

Table 1: GFI EventsManager engines

Engine	Description
The Event Retrieval Engine	Used to collect Windows® Event Logs and Text Logs from networked event sources. During the Event Collection process this engine will: 1. Log-on to the event source(s) 2. Collect events from the source(s) 3. Send collected events to GFI EventsManager Server 4. Log-off from the event source(s). The Event Retrieval Engine collects events at specific time intervals. The event collection interval is configurable from the GFI EventsManager management console
The SQL Server® Listener	The listener receives trace messages from the scanned Microsoft® SQL Server® in real time. On receipt, GFI EventsManager processes the message immediately.
The Oracle Retrieval Engine	The Oracle Retrieval Engine connects periodically to Oracle servers and collects audits from a specific auditing table. Similar to the Microsoft® Windows® Event Retrieval Engine, GFI EventsManager processes events generated by the Oracle server.
Log Receiving Engine	The Event Receiving Engine acts as a Syslog and an SNMP Traps server; it listens and collects Syslog and SNMP Trap events/messages sent by various sources on the network. As opposed to the Event Retrieval Engine, the Event Receiving Engine receives messages directly from the event source; therefore it does not require to remotely log-on to the event sources for event collection. Further to this, Syslog and SNMP Trap events/messages are collected in real-time and therefore no collection time intervals need to be configured. By default, the Event Receiving Engine listens to Syslog messages on port 514 and to SNMP Trap messages on port 162. Both port settings are however customizable via the GFI EventsManager management console.

1.2.2 Stage 2: Event Processing

During this stage, GFI EventsManager will run a set of Event Processing Rules against collected events. Event Processing rules are instructions that:

- Analyze the collected logs and classify processed events as Critical, High, Medium, Low or Noise (unwanted or repeated events)
- Filter events that match specific conditions
- Trigger email, SMS and network alerts on key events
- Trigger remediation actions such as the execution of executable files or scripts on key events
- Optionally archive collected events in the database backend.

GFI EventsManager can be configured to archive events without running events processing rules. In such cases, even though no rules are applied against collected logs, archiving is still handled at the Event Processing stage. For more information refer to Events Processing Rules.

Important

Some of the key modules in GFI EventsManager must run under administrative privileges. For more information on these modules refer to the following article: http://go.gfi.com/?pageid=esm_process_rights

1.3 Conventions used in this guide

The table below describes the common terms and conventions used in this Guide:

Table 2: Terms and conventions used in this manual

Term	Description
	Additional information and references essential for the operation of GFI EventsManager.
	Important notifications and cautions regarding potential issues that are commonly encountered.
>	Step by step navigational instructions to access a specific function.
Bold text	Items to select such as nodes, menu options or command buttons.
Italics text	Parameters and values that you must replace with the applicable value, such as custom paths and filenames.
`Code`	Indicates text values to key in, such as commands and addresses.

2 Installing GFI EventsManager

This chapter describes the possible deployment scenarios supported by GFI EventsManager. It is essential to review system requirements and computer settings prior to installing the product to ensure full communication between GFI EventsManager and the network devices/computers that must be monitored.

Topics in this chapter:

2.1 Deployment scenarios 26

2.2 System requirements 32

2.3 Upgrading GFI EventsManager 35

2.4 Installing a new instance of GFI EventsManager 44

2.5 Testing the installation 53

2.1 Deployment scenarios

GFI EventsManager can be installed on any computer which meets the minimum system requirements irrespective of the location on your network. If you want to collect event logs from Microsoft® Windows® Vista or later operating systems, GFI EventsManager must be installed on a machine running Microsoft® Windows® Vista, 7 or Server 2008.

Use GFI EventsManager to manage event logs generated by:

- The same computer where it is installed
- All the servers, workstations and network devices that are reachable from the computer on which it is installed on.

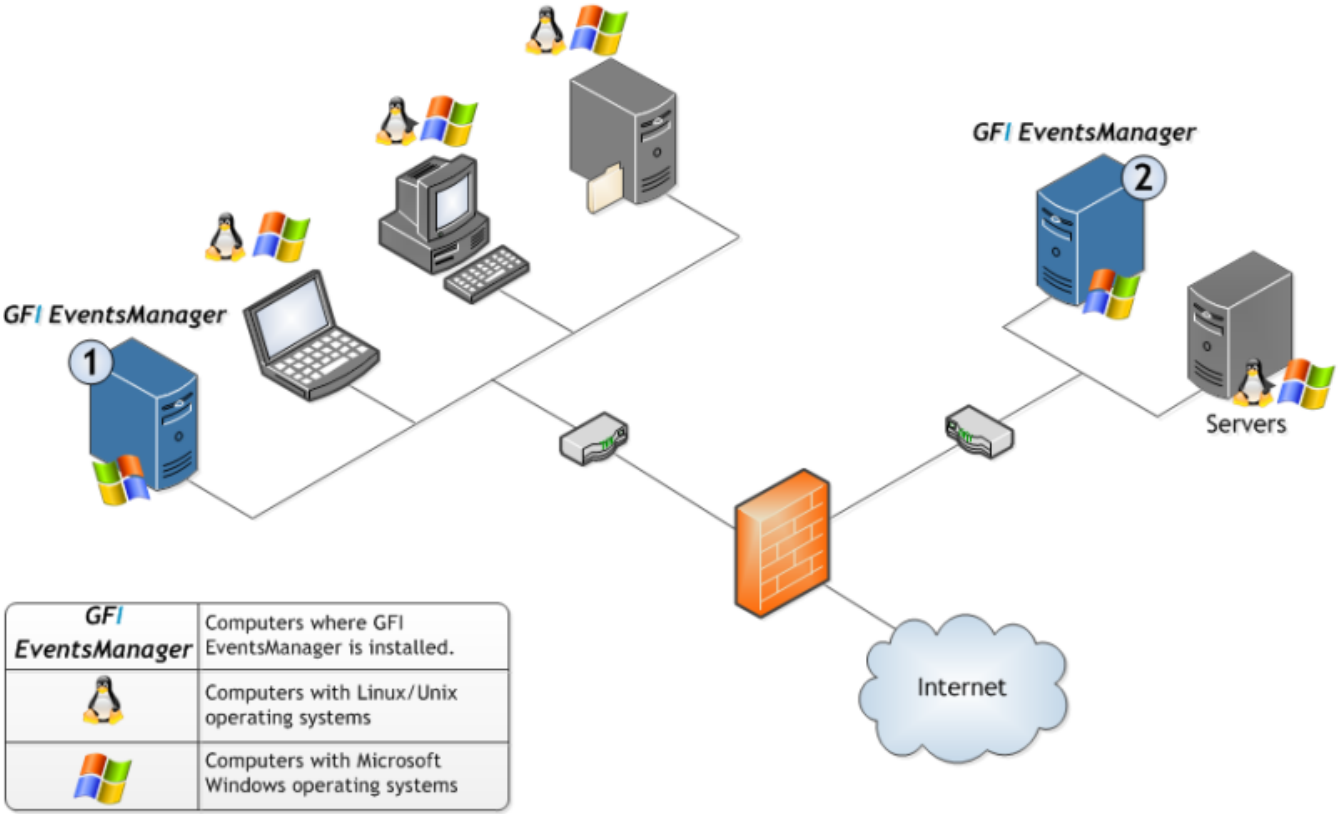


Figure 1: GFI EventsManager deployment scenario

This section contains information about deploying GFI EventsManager in a:

- Local Area Network (LAN) - Monitor activity of the main production network, servers and work-stations
- Demilitarized Zone (DMZ) - Monitor events generated by public service servers, such as mail servers, web servers and DNS servers
- Wide Area Network (WAN) - Monitor events generated by computers and network devices spread across different geographical locations.

2.1.1 Installing GFI EventsManager in a Local Area Network (LAN)

GFI EventsManager can be deployed on Windows® based networks as well as on mixed environments where Linux and Unix systems are being used as well.

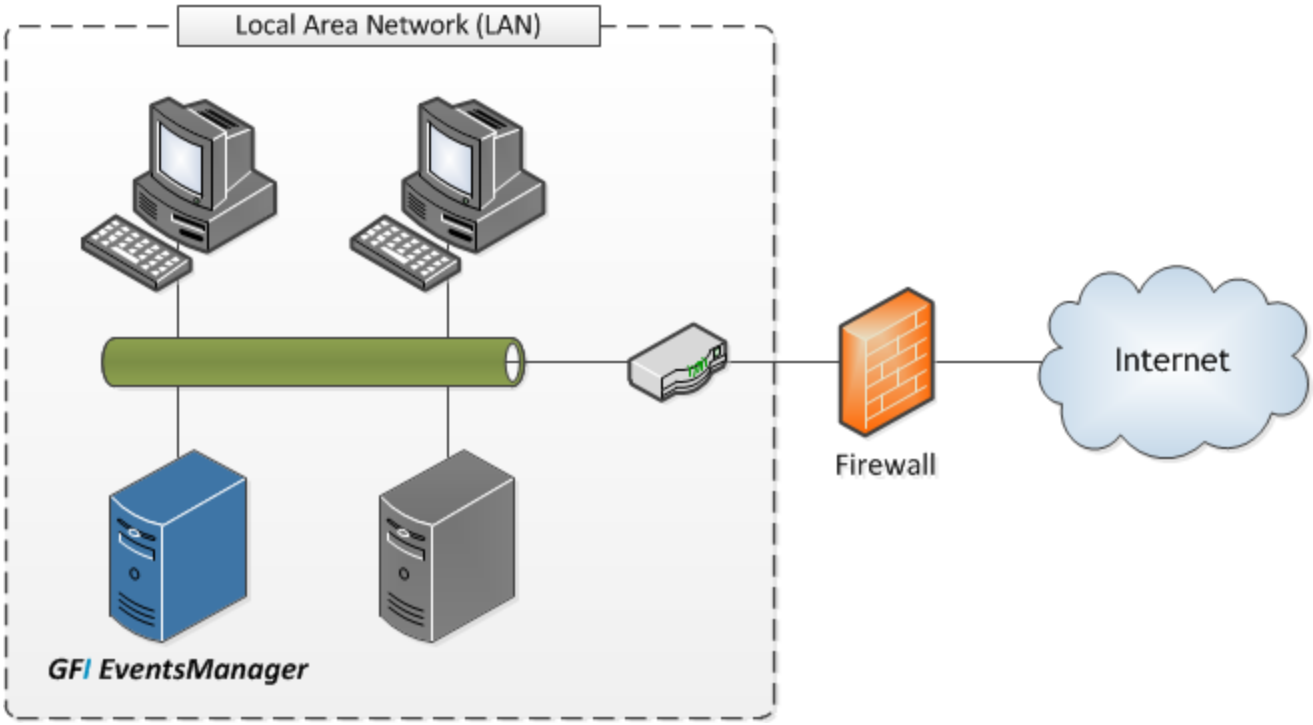


Figure 2: Deployment of GFI EventsManager in LAN

When installed on a Local Area Network (LAN) GFI EventsManager can manage Windows® events, Text Logs, Syslog messages, SNMP Trap and SQL Server® audit messages generated by any hardware or software that is connected to the LAN, including:

Table 3: Devices supported by GFI EventsManager

Device	Example
Workstations and laptops	End-user computers and systems.
Servers	Web servers, Mail servers, DNS servers and more.
Network devices	Routers, switches and any other device that generates performance logs.
Software	Including GFI EndPointSecurity, GFI LanGuard and other applications that generate logs.
Specialized Services	Microsoft® Internet Information Server – IIS.
PABXs, Keyless Access Systems, Intrusion detections systems and more	GFI EventsManager enables you to monitor any device that is attached to the network.

2.1.2 GFI EventsManager within a Demilitarized Zone (DMZ)

GFI EventsManager is able to monitor events generated by machines in a DMZ, from being installed within the LAN or by being installed directly in the DMZ. Since a firewall or a router usually protects this zone with network traffic filtering capabilities, you must make sure that:

- The communication ports used by GFI EventsManager are not blocked by the firewall. For more information on the communication ports used by GFI EventsManager refer to: http://go.gfi.com/?pageid=esm_ports.
- GFI EventsManager has administrative privileges over the computers that are running on the DMZ.

Important

GFI recommends to install GFI EventsManager directly in the DMZ as opposed to enabling firewall ports and permissions to allow communication between LAN and DMZ computers, servers and network devices.

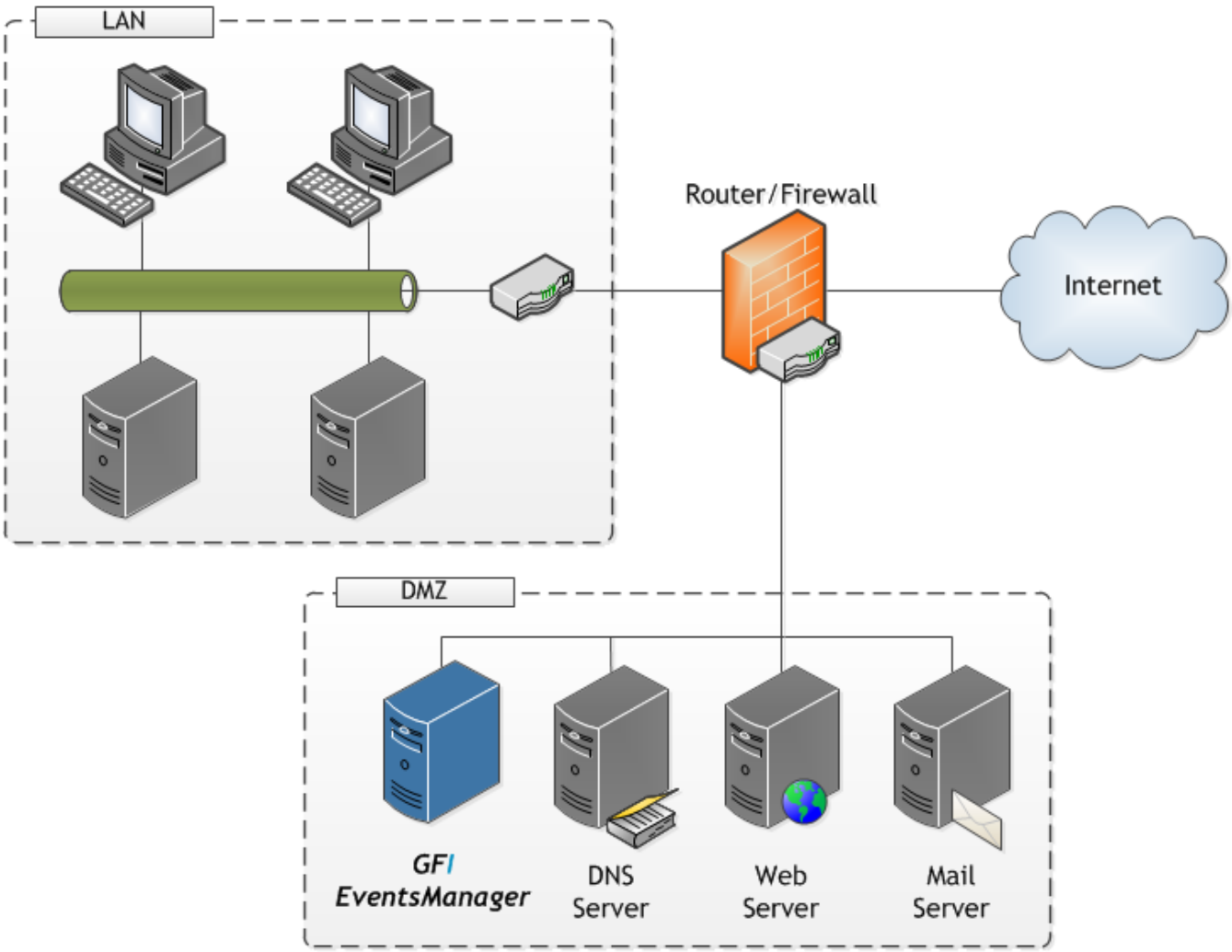


Figure 3: The DMZ sits between the internal LAN and the Internet

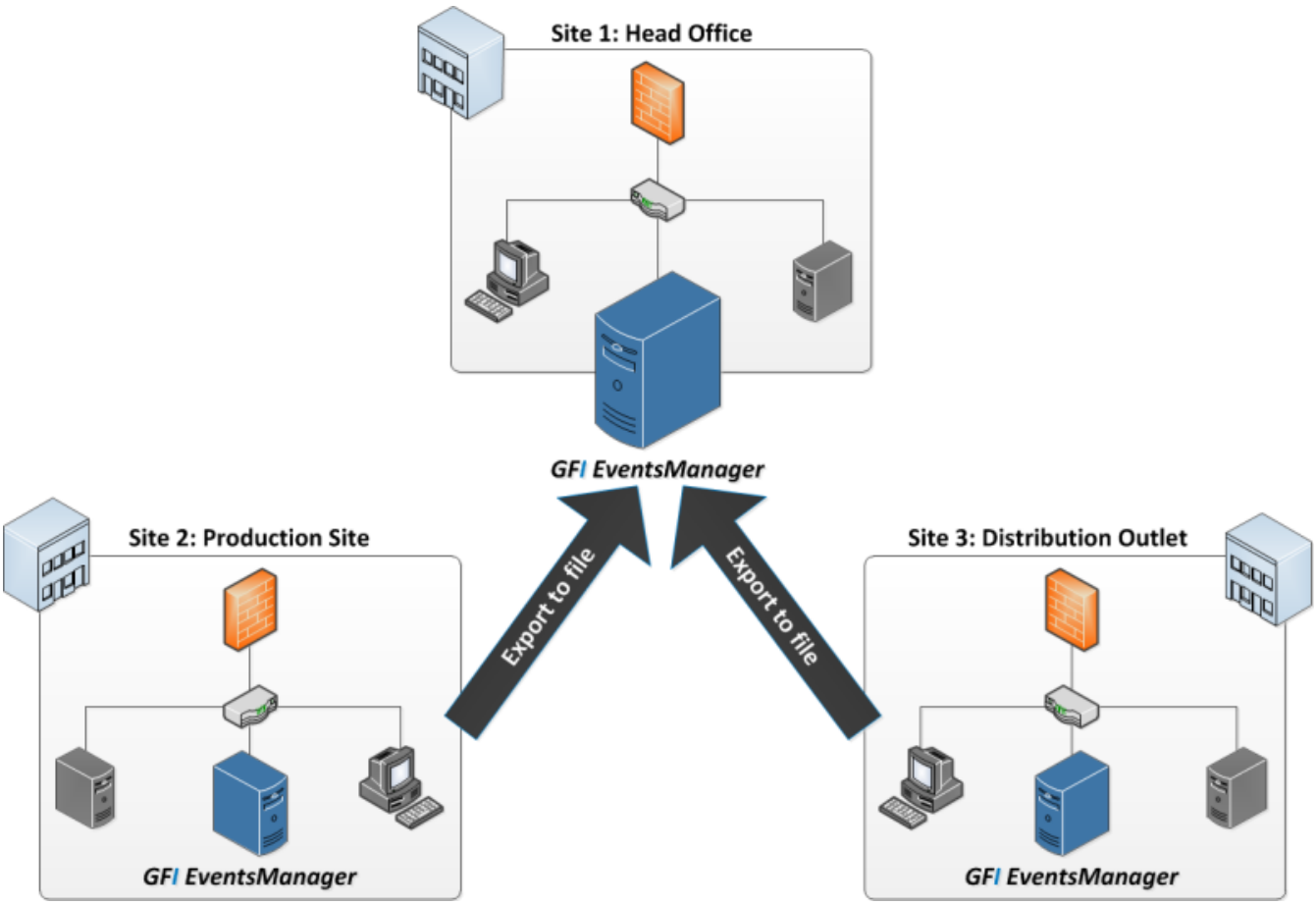
A DMZ is the neutral network which sits between the "internal" corporate network and the "outside world" (Internet). The deployment of GFI EventsManager in a DMZ helps you automate the management of events generated by DMZ hardware and software systems; such as:

Table 4: Benefits of installing GFI EventsManager in DMZ

DMZ Automation	Description
Automate management of Web and Mail server events	DMZ networks are normally used for the running of hardware and software systems that have Internet specific roles such as HTTP servers, FTP servers, and Mail servers. Hence, you can deploy GFI EventsManager to automatically manage the events generated by: » Web-servers including the W3C web-logs generated by Apache web-servers on LAMP web platforms » Windows® based web-servers including the W3C web-logs generated by Microsoft® Internet Information Servers (IIS) » Linux/Unix and Windows® based mail-servers including the Syslog auditing services messages generated by Sun Solaris v. 9 or later » Automate management of DNS server events » If you have a public DNS server, there's a good chance that you are running a DNS server on the DMZ. Hence you can useGFI EventsManager to automatically collect and process DNS server events including those stored in your Windows® DNS Server logs.
Automate management of DNS server events	If you have a public DNS server, there's a good chance that you are running a DNS server on the DMZ. Hence you can use GFI EventsManager to automatically collect and process DNS server events including those stored in your Windows® DNS Server logs.
Automate management of network appliance events	Routers and firewalls are two network appliances commonly found in a DMZ. Specialized routers and firewalls (example: Cisco IOS series routers) not only help protect your internal network, but provide specialized features such as Port Address Translation (PAT) that can augment the operational performance of your systems. By deploying GFI EventsManager on your DMZ, you can collect the events generated by such network appliances. For example, you can configure GFI EventsManager to act as a Syslog Server and collect in real-time the Syslog messages generated by Cisco IOS routers.

2.1.3 GFI EventsManager within a Wide Area Network (WAN)

GFI EventsManager can be installed in environments that have multiple sites in different geographical locations.



Screenshot 3: Export data from remote sites to the main instance of GFI EventsManager

This is achieved by installing an instance of GFI EventsManager at each location. Periodically (based on a schedule), you can export events from the remote sites and import them into the central database for complete consolidation of event logs.

Events for the remote site can then be viewed through the Events Browser. Reports with information relevant to remote sites can also be generated using data from the central database. Use the Switch Database option to view or report on information stored on remote databases.

Note

For more information refer to Switching File Storage Databases.

Note

For more information refer to Database Maintenance.

2.2 System requirements

To install GFI EventsManager, the host computer must meet the system requirements specified below. If you plan to manage a large number of event sources in a high traffic network, consider using a computer with greater system specs. Refer to the following sections for information about:

- Hardware requirements
- Supported operating systems (32-bit and 64-bit)
- Other software components
- Storage requirements
- Firewall ports and protocols
- Firewall permissions
- Event source settings
- Antivirus exceptions
- Computer identification considerations
- Collecting event logs from computers running Microsoft® Vista or later

2.2.1 Hardware requirements

The following table contains hardware requirements for GFI EventsManager:

Table 5: Hardware requirements

Hardware Component	Specification
Processor	2.5 GHz dual core or higher.
RAM	3 GB.
Hard disk	10 GB free space.

Note

Hard disk size depends on your environment, the size specified in the requirements is the minimum required to install and archive events.

2.2.2 Supported operating systems (32-bit and 64-bit)

GFI EventsManager can be installed on a computer running any of the following operating systems:

- Windows® Server 2012 - Foundation, Essentials, Standard or Datacenter
- Windows® Server 2008 - Standard or Enterprise
- Windows® Server 2008 R2 – Standard or Enterprise
- Windows® Server 2003 SP2 - Standard or Enterprise
- Windows® 8 - Standard, Professional or Enterprise
- Windows® 7 - Enterprise, Professional or Ultimate
- Windows® Vista SP1 - Enterprise, Business or Ultimate
- Windows® XP Professional SP3

- Windows® SBS 2008
- Windows® SBS 2003.

> **Note**
>
> GFI EventsManager cannot be installed on Server Core Installations.

2.2.3 Other software components

The additional software components below are recommended to be installed to ensure full functionality of GFI EventsManager:

- Microsoft® .NET framework 4.0
- Microsoft® Data Access Components (MDAC) 2.8 or later
- A mail server (when email alerting is required).

> **Note**
>
> Microsoft® Data Access Components (MDAC) 2.8 can be downloaded from http://go.gfi.com/?pageid=esm_mdac

2.2.4 Storage requirements

The storage requirements below are based on the average size of an event log, being 535 bytes per event. The following specifications indicate the required hard disk size, that caters for your infrastructure's requests:

Table 6: Storage space requirements

Hard Disk Space	Number of Events
Events stored per 1 Gb of storage space	2,006,994
Events stored in 500 Gb of storage space	1,003,497,032

2.2.5 Firewall ports and protocols

The following table contains ports and protocols that must be allowed by the firewall of the GFI EventsManager host:

Table 7: Firewall ports and protocols

Port	Protocols	Description
135	UDP and TCP	Target machines use this port to publish information regarding available dynamic ports. GFI EventsManager uses this information to be able to communicate with the target machines.
139 and 445	UDP and TCP	Used by GFI EventsManager to retrieve the event log descriptions from target machines.
162	UDP and TCP	Used by GFI EventsManager to receive SNMP traps. Ensure that this port is open on the machine where GFI EventsManager is installed.
514	UDP and TCP	Used by GGFI EventsManager to receive SYSLOG messages.
1433	UDP and TCP	Used by GFI EventsManager to communicate with the SQL Server® database backend. Ensure that this port is enabled on Microsoft® SQL Server® and on the machine where GFI EventsManager is installed.

Port	Protocols	Description
1521	UDP and TCP	Used to collect Oracle Server audit logs. Port 1521 is the default port for this connection. If the port is changed manually in the Oracle Listener's configuration, adjust firewall settings accordingly.
49153	UDP and TCP	Used by GFI EventsManager to collect events from event sources with Microsoft® Windows®Vista or Microsoft® Windows® 7.

2.2.6 Firewall permissions

The following table contains permissions that must be allowed by the firewall of the GFI EventsManager host:

Table 8: Firewall permissions

Firewall Permissions and Audit Policies	Windows® Server 2008	Windows® Server 2003	Windows® XP	Windows® 7	Windows® Vista
Remote Event Log Management	Enable	Not applicable	Not applicable	Enable	Enable
File and Printer sharing	Enable	Enable	Enable	Enable	Enable
Network discovery	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Object access	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Process tracking	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Audit account management	Enable	Enable	Enable	Enable	Enable
Audit policy: Audit system events	Enable	Enable	Enable	Enable	Enable

Note

For more information, refer to Enabling permissions on events sources manually or Enabling permissions on event sources automatically.

2.2.7 Event source settings

The following table contains settings that must be configured on your event sources. Event sources are computers that you want to monitor by GFI EventsManager:

Table 9: Event source settings

Log Type	Description
Windows® event log processing	Enable remote registry.
Text log processing	The source folders must be accessible via Windows® shares.
Syslog and SNMP Traps processing	Configure sources/senders to send messages to the computer/IP where GFI EventsManageris installed.
Scanning machines with Windows® Vista or later	Install GFI EventsManager on a computer running Windows® Vista or later.
System auditing	Enable auditing on event sources. For information, refer to Enabling event source permissions manually and Enabling event source permissions automatically.

2.2.8 Antivirus exceptions

If an antivirus application installed on the computer where GFI EventsManager is running, make sure that:

- Traffic is not blocked on the ports in use by GFI EventsManager
- **esmui.exe** and **esmproc.exe** are allowed access through the firewall(s)
- GFI EventsManager folders are excluded from real-time antivirus scanning.

2.2.9 Computer identification considerations

GFI EventsManager identifies computers via computer name or IP. If NETBIOS-compatible computer names are used, ensure that your DNS service is properly configured for name resolution. Unreliable name resolution downgrades overall system performance. If you disable NETBIOS over TCP/IP, you can still use GFI EventsManager, however you must specify computer name by IP.

2.2.10 Collecting event logs from computers running Microsoft® Vista or later

GFI EventsManager cannot be installed on Microsoft® Windows® XP to monitor events of Microsoft® Windows® Vista or later. Microsoft® Windows® Vista and Microsoft® Windows® 7 introduced extensive structural changes in event logging and event log management. The most important of these changes include:

- A new XML-based format for event logs. This provides a more structured approach to reporting on all system occurrences.
- Event categorization in four distinct groups: Administrative, Operational, Analytic and Debug
- A new file format (evtx) that replaces the old evt file format.

Due to these changes, to collect and process event logs from Microsoft® Windows® Vista or later, GFI EventsManager must be installed on a system running:

- Windows® Vista
- Windows® 7
- Windows® Server 2008.

Note

Windows® XP events can be collected when GFI EventsManager is installed on Windows® Vista or later machines.

Note

When GFI EventsManager is using a non-domain account to collect events from Windows® Vista machines or later, target machines must have User Account Control (UAC) disabled. For more information refer to Disabling User Account Control (UAC).

2.3 Upgrading GFI EventsManager

Upgrading from versions older than GFI EventsManager 2011 is not fully supported. Some settings may be lost due to the underlying technology changes. GFI EventsManager can be upgraded using any of the following methods:

Table 10: Upgrading GFI EventsManager

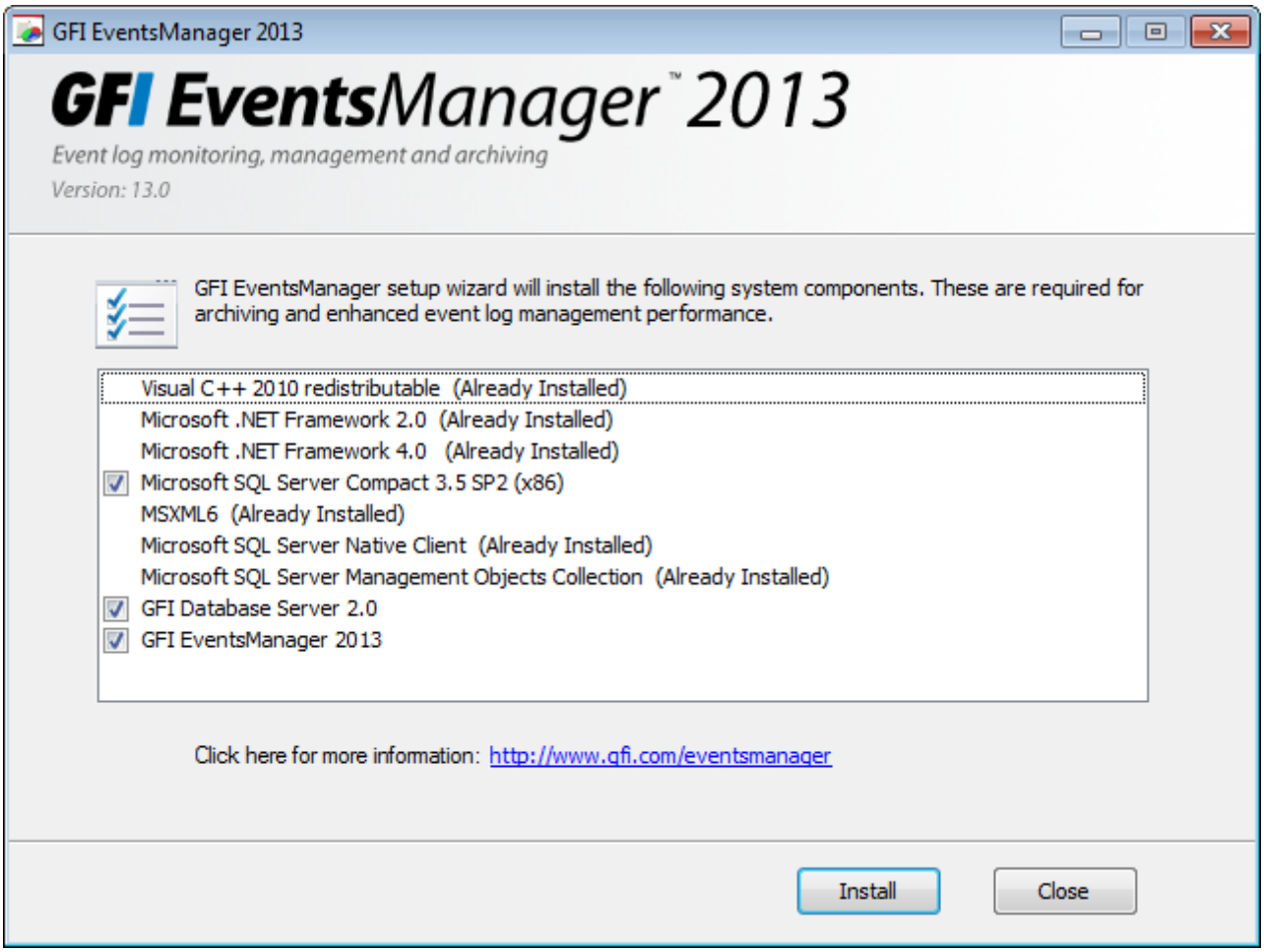
Method	Description
Automatically	Launch the new setup and complete the wizard to upgrade and retain data. For more information refer to Upgrading from a previous version.
Manually	Export settings and events from an older version of GFI EventsManager and import them in the new one using Database Operations and Import/Export tools. For more information refer to Creating Maintenance Jobs and Importing and Exporting Settings.

2.3.1 Upgrading from a previous version

> **Note**
>
> Before starting the upgrade, disable any anti-virus software running on the system.

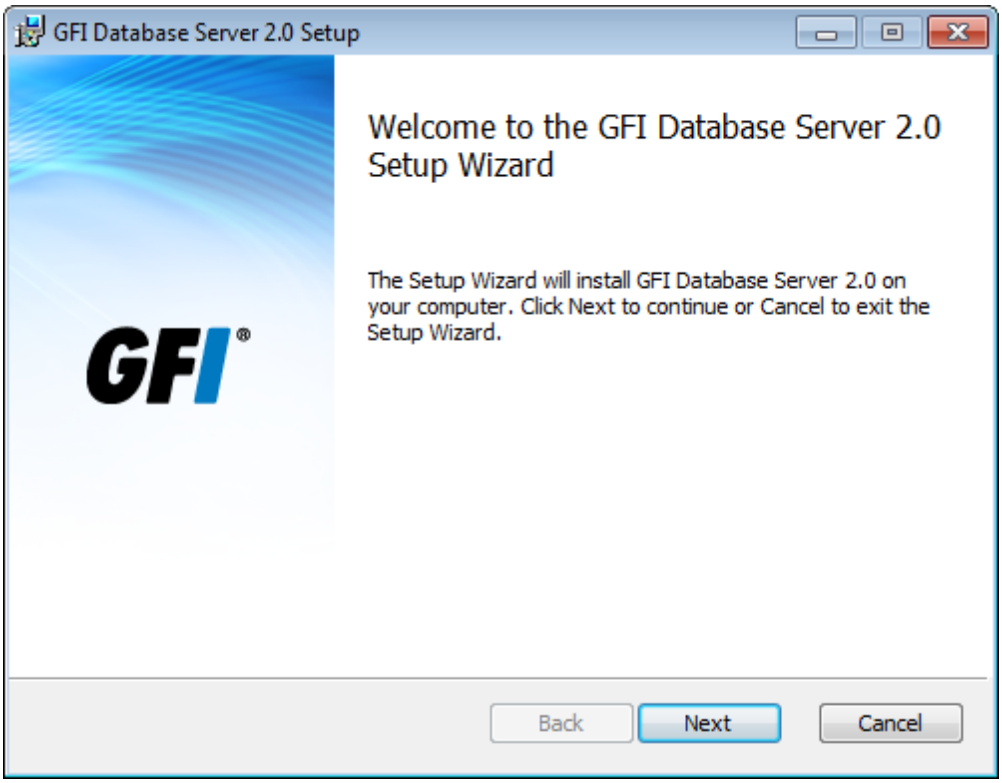
To upgrade to a new version:

1. Double-click **EventsManager.exe**.


GFI EventsManager 2013
GFI EventsManager 2013
Event log monitoring, management and archiving
Version: 13.0
GFI EventsManager setup wizard will install the following system components. These are required for archiving and enhanced event log management performance.
Visual C++ 2010 redistributable (Already Installed)
Microsoft .NET Framework 2.0 (Already Installed)
Microsoft .NET Framework 4.0 (Already Installed)
Microsoft SQL Server Compact 3.5 SP2 (x86)
MSXML6 (Already Installed)
Microsoft SQL Server Native Client (Already Installed)
Microsoft SQL Server Management Objects Collection (Already Installed)
GFI Database Server 2.0
GFI EventsManager 2013
Click here for more information: http://www.gfi.com/eventsmanager
Install
Close

Screenshot 4: Upgrade prerequisite check

2. The installer displays a list of system components that must be installed prior to installing the product. Click **Install** to start the installation of missing system components (if necessary).


GFI Database Server 2.0 Setup
Welcome to the GFI Database Server 2.0 Setup Wizard
The Setup Wizard will install GFI Database Server 2.0 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
GFI
Back
Next
Cancel

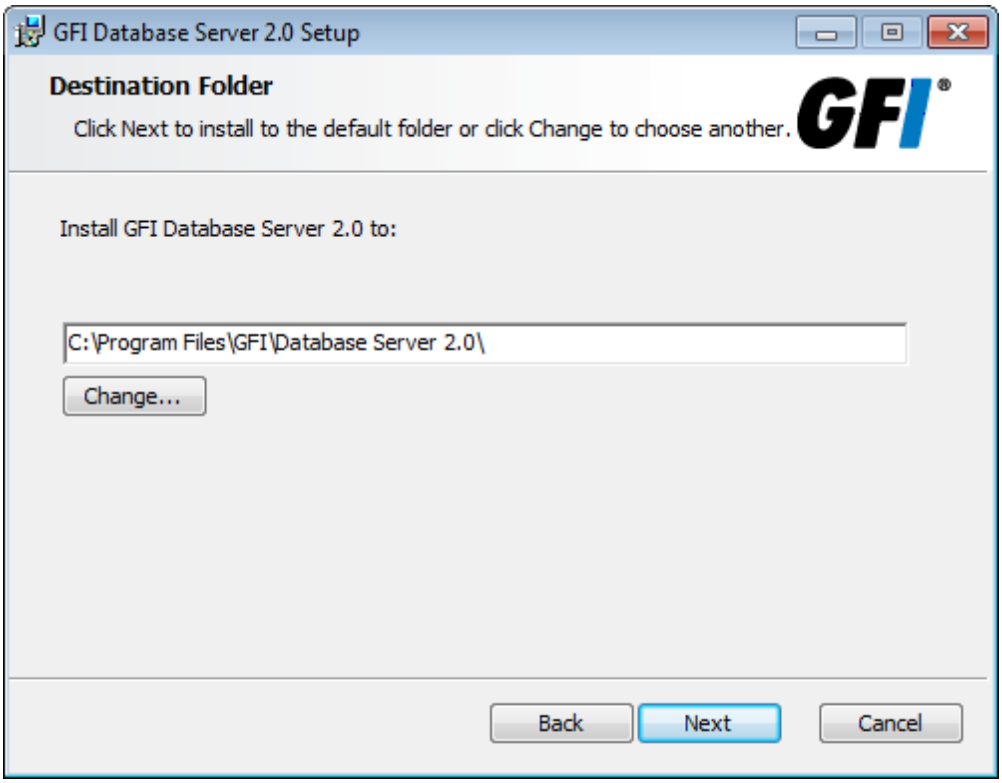
Screenshot 5: DLib Database Server

3. The DLib Database Server install wizards opens automatically after system components are installed. Click **Next** at the wizard welcome screen.

GFI Database Server 2.0 Setup
End-User License Agreement
Please read the following license agreement carefully
GFI
GFI® End-User License Agreement
For: GFI FaxMaker®; GFI MailArchiver®, GFI MailEssentials® and GFI MailSecurity®; GFI WebMonitor®; GFI LanGuard®;
GFI Network Server Monitor®; GFI EventsManager®; GFI BackUp®; GFI Device Warden™ and GFI EndPointSecurity®
("Software")
I accept the terms in the License Agreement
Print
Back
Next
Cancel

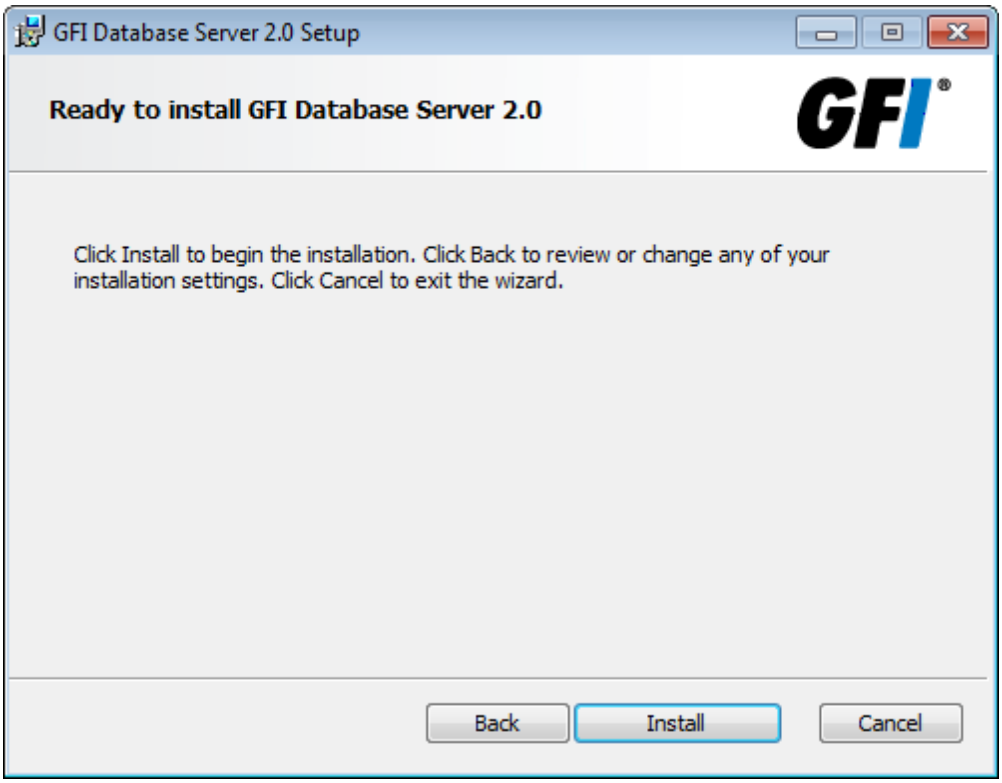
Screenshot 6: DLib Database Server EULA

4. Carefully read the license agreement. Select **I accept the terms in the License Agreement** and click **Next**.



Screenshot 7: DLib install folder

5. Click **Next** to install the database server in the default folder or click **Change...** to select an alternate folder where it is installed.


GFI Database Server 2.0 Setup
Ready to install GFI Database Server 2.0
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

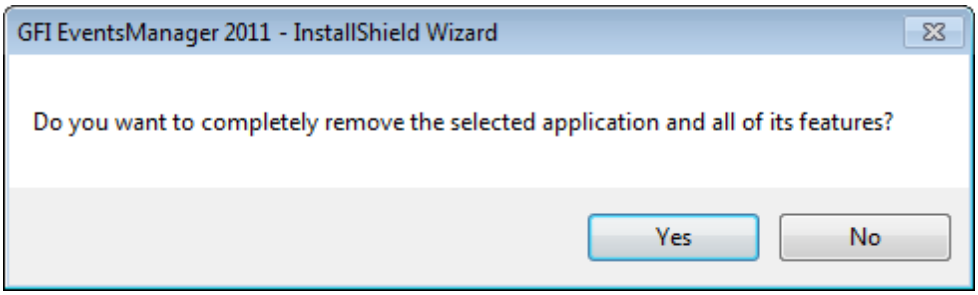
Screenshot 8: Start installing DLib Database Server

6. Click **Install** to start installing DLib Database Server. Click **Finish** when prompted.

> **Note**
>
> After the database server is installed, the installer automatically opens the install wizard of GFI EventsManager Management Console.

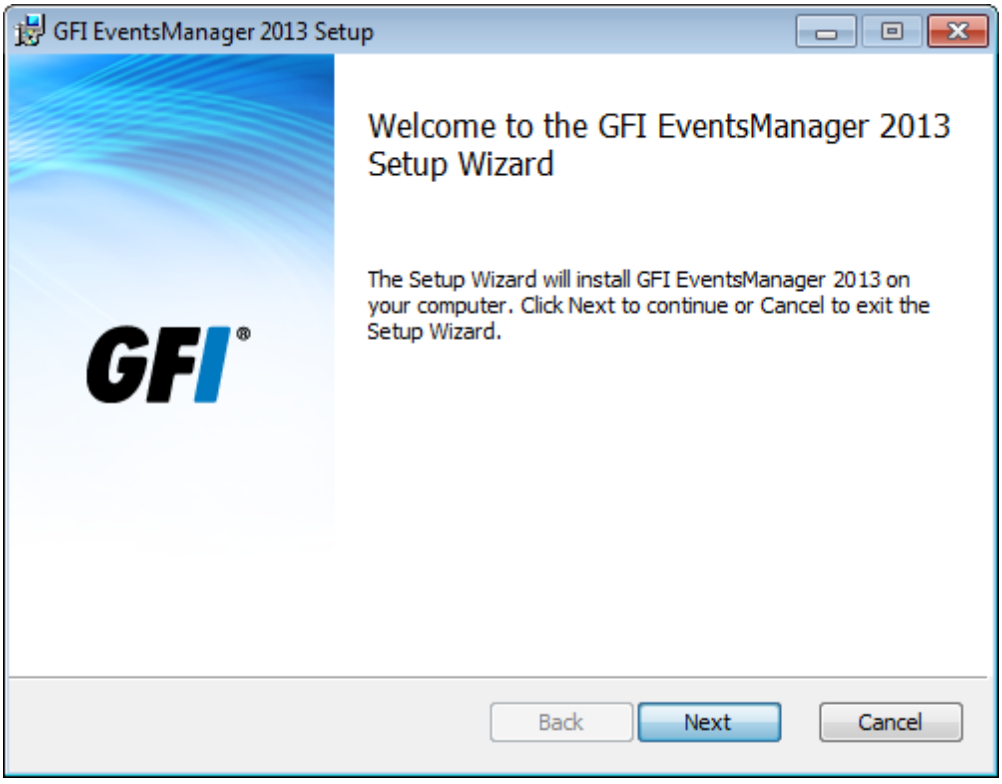
7. Click **Yes** to uninstall the previous version of GFI EventsManager and continue installing the new one. Click **No** to stop the installation.

> **Note**
>
> Running two instances of the Management Console on the same computer is not supported.


GFI EventsManager 2011 - InstallShield Wizard
Do you want to completely remove the selected application and all of its features?
Yes
No

Screenshot 9: Delete old version files

8. Click **Yes** to confirm the deletion of files from the older version of GFI EventsManager or click **No** to stop the installation.


GFI EventsManager 2013 Setup
Welcome to the GFI EventsManager 2013 Setup Wizard
The Setup Wizard will install GFI EventsManager 2013 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
GFI
Back
Next
Cancel

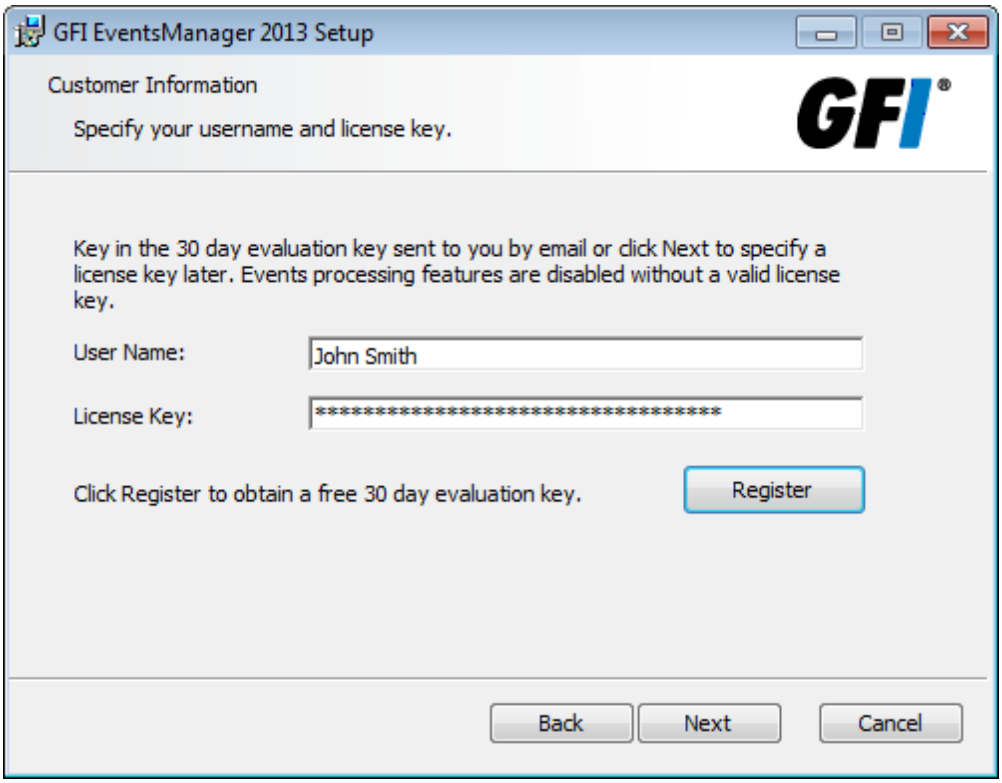
Screenshot 10: GFI EventsManager setup wizard welcome screen

9. Click **Next** at the welcome screen of the GFI EventsManager setup wizard.

GFI EventsManager 2013 Setup
End-User License Agreement
Carefully read the following end user license agreement
GFI End-User License Agreement
For: GFI FaxMaker™; GFI MailArchiver™, GFI MailEssentials™ and GFI MailSecurity™; GFI WebMonitor™; GFI LanGuard™;
GFI Network Server Monitor™; GFI EventsManager™; GFI BackUp™; GFI Device Warden™ and GFI EndPointSecurity™
("Software")
I accept the terms in the License Agreement
Print
Back
Next
Cancel

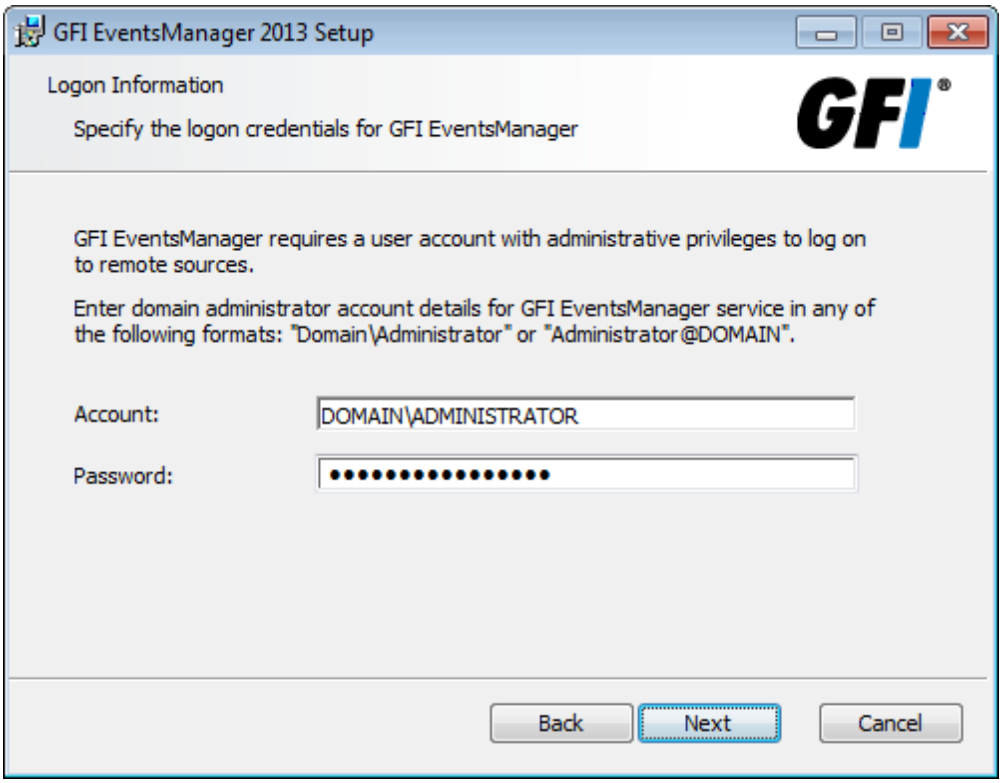
Screenshot 11: GFI EventsManager EULA

10. Carefully read the license agreement. Select **I accept the terms in the License Agreement** and click **Next**.


GFI EventsManager 2013 Setup
Customer Information
Specify your username and license key.
Key in the 30 day evaluation key sent to you by email or click Next to specify a license key later. Events processing features are disabled without a valid license key.
User Name:
John Smith
License Key:
Click Register to obtain a free 30 day evaluation key.
Register
Back
Next
Cancel

Screenshot 12: GFI EventsManager registration details

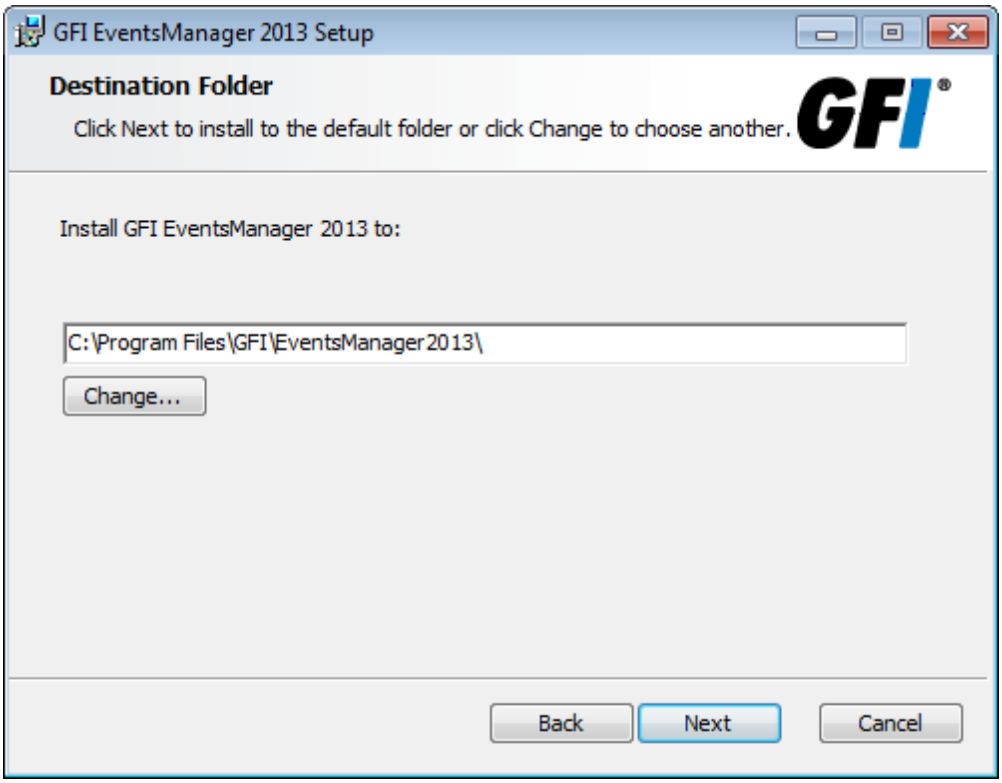
11. Key in your user name and license key in the **User Name** and **License Key** fields. To register for a free 30 day evaluation license key, click **Register**. Click **Next**.


GFI EventsManager 2013 Setup
Logon Information
Specify the logon credentials for GFI EventsManager
GFI
GFI EventsManager requires a user account with administrative privileges to log on to remote sources.
Enter domain administrator account details for GFI EventsManager service in any of the following formats: "Domain\Administrator" or "Administrator@DOMAIN".
Account:
DOMAIN\ADMINISTRATOR
Password:
Back
Next
Cancel

Screenshot 13: Remote logon credentials for event log monitoring

12. Key in the logon credentials that GFI EventsManager uses to log onto remote computers.

> **Note**
>
> It is recommended to use a domain administrator or an account with administrative rights over all the remote computers managed by GFI EventsManager.



Screenshot 14: GFI EventsManager install folder

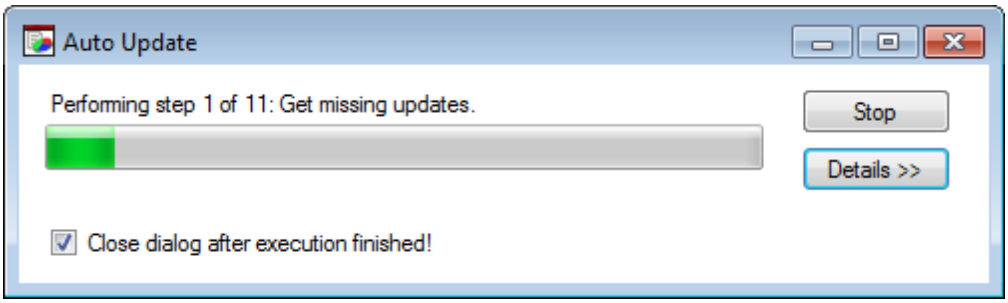
13. Click **Next** to install the Management Console in the default folder or click **Change...** to select an alternate folder where it is installed.

GFI EventsManager 2013 Setup
Ready to install GFI EventsManager 2013
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

Screenshot 15: GFI EventsManager installation completed

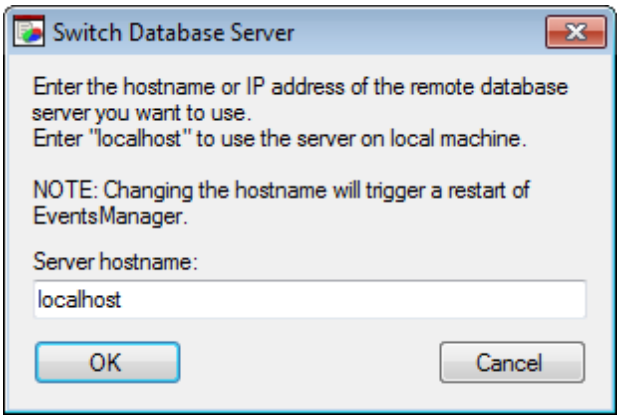
14. Click **Install** to start the installation.

15. When the installation is complete, click **Finish**.



Screenshot 16: Auto updates check

16. If GFI EventsManager detects an Internet connection, it automatically attempts to download product updates from GFI updates servers. Click **Details** to expand the information section of the Auto Update dialog and view the updates that are being downloaded.


Switch Database Server
Enter the hostname or IP address of the remote database server you want to use.
Enter "localhost" to use the server on local machine.
NOTE: Changing the hostname will trigger a restart of EventsManager.
Server hostname:
localhost
OK
Cancel

Screenshot 17: Set the database backend

> **Note**
>
> After product updates are applied, the **Switch Database Server** dialog opens. This dialog is used to link the Management Console to a database server. You can switch database servers from the Management Console. For more information refer to Switching between file storage databases.

17. Specify the computer that has D-Lib Database Server installed on it. If the database you want to use is on:

- The localhost - key in **localhost** (default)
- A remote computer - key in the **computer name** or **IP address**.

Click **OK**.

> **Note**
>
> Once the installation is complete, the Management Console opens automatically. To launch it manually, click **Start > All Programs > GFI EventsManager > Management Console**.

Note

Configuration data of GFI EventsManager 2012 is not deleted. Data is copied to the new install folder (*%install folder%*\Data_Old). Data in this folder is used to retain previous configurations.

Note

Test the installation to ensure that all the components were successfully installed. For more information refer to Testing the installation.

2.4 Installing a new instance of GFI EventsManager

The components listed in the following table can be installed using **EventsManager.exe**:

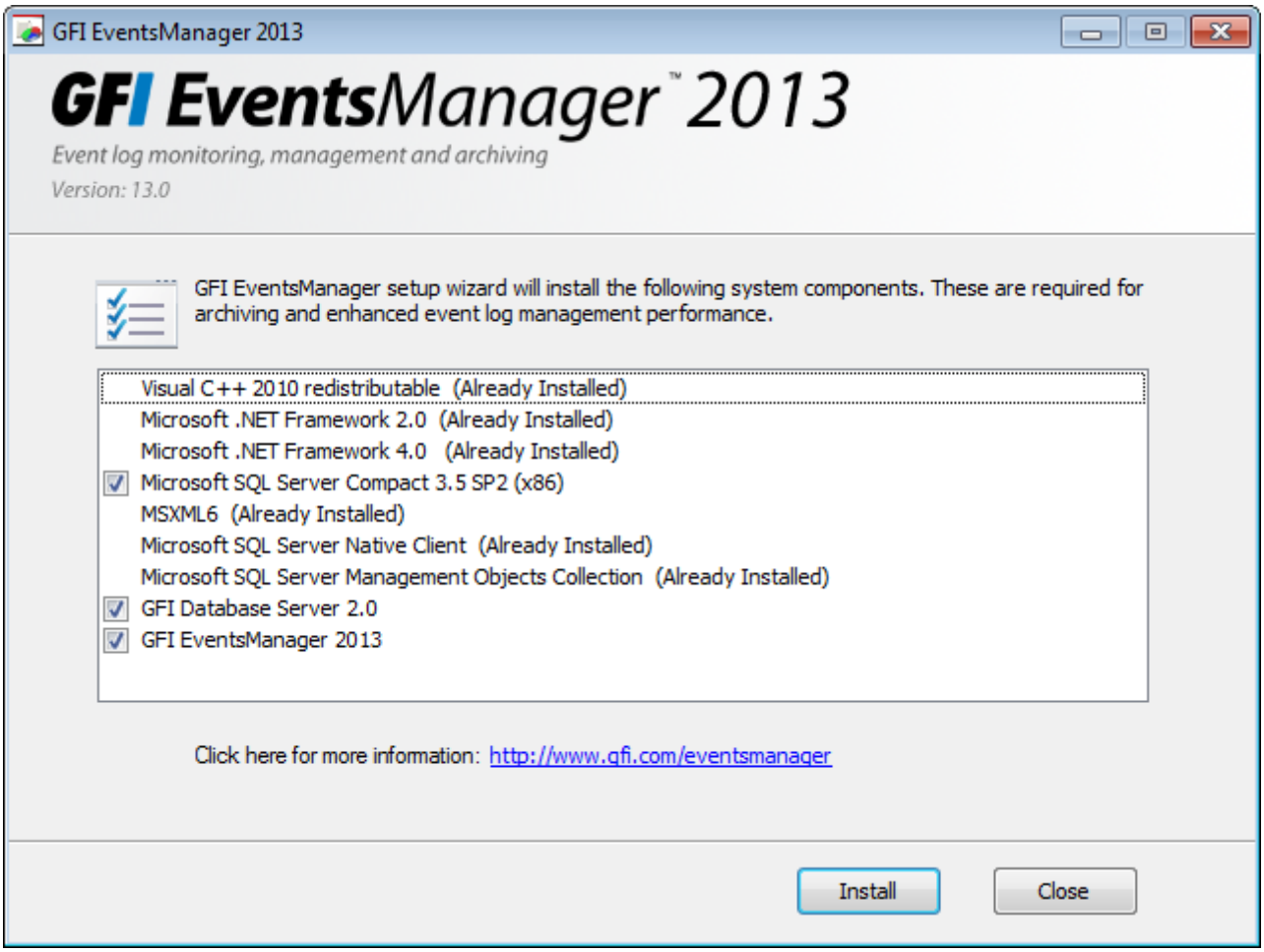
Table 11: Components installed using EventsManager.exe

Component	Description
System components	The following system components are required by GFI EventsManager for complete functionality: » Visual C++ 2010 redistributable » Microsoft® .NET Framework 2.0 » Microsoft® .NET Framework 4.0 » Microsoft® SQL Server® Compact 3.5 SP2 » MSXML6 » Microsoft® SQL Server® Native Client » Microsoft® SQL Server® Management Objects Collection.
DLib Database Server	DLib Database Server is the component where GFI EventsManager stores processed logs. The database server can be installed on the same computer that is running GFI EventsManager as well as on a separate remote computer or network drive.
GFI EventsManager	The actual product from where you can manage and monitor events generated by computers and devices in your network.

2.4.1 Installation procedure

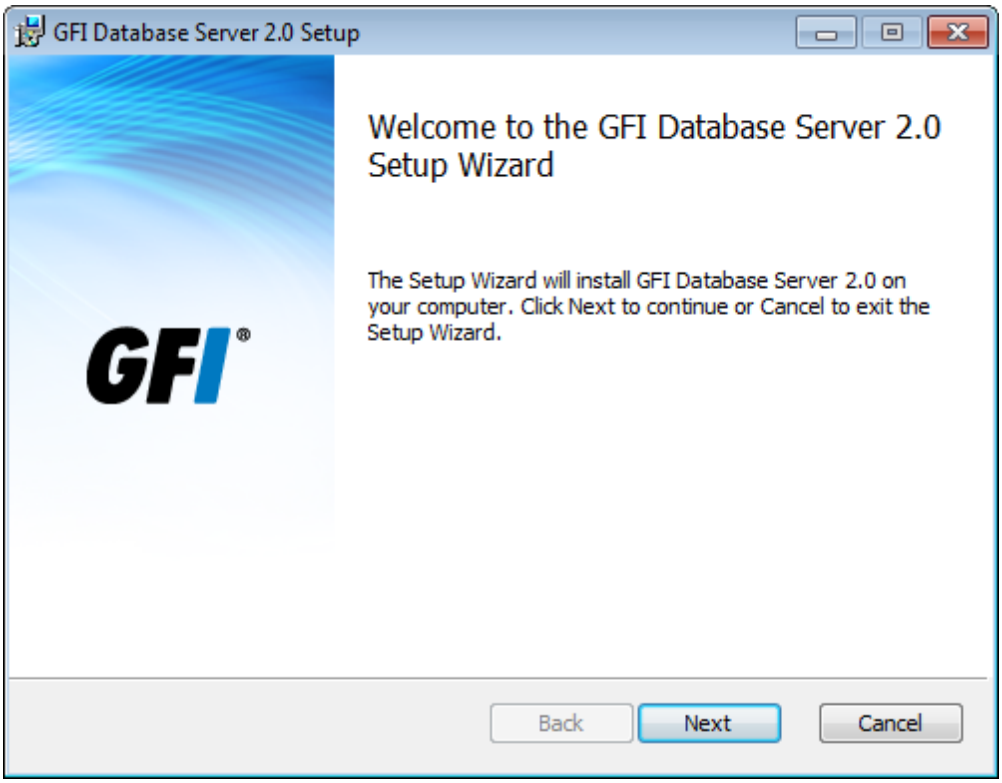
To install GFI EventsManager:

1. Double-click **EventsManager.exe**.


GFI EventsManager 2013
GFI EventsManager 2013
Event log monitoring, management and archiving
Version: 13.0
GFI EventsManager setup wizard will install the following system components. These are required for archiving and enhanced event log management performance.
Visual C++ 2010 redistributable (Already Installed)
Microsoft .NET Framework 2.0 (Already Installed)
Microsoft .NET Framework 4.0 (Already Installed)
Microsoft SQL Server Compact 3.5 SP2 (x86)
MSXML6 (Already Installed)
Microsoft SQL Server Native Client (Already Installed)
Microsoft SQL Server Management Objects Collection (Already Installed)
GFI Database Server 2.0
GFI EventsManager 2013
Click here for more information: http://www.gfi.com/eventsmanager
Install
Close

Screenshot 18: Upgrade prerequisite check

2. The installer displays a list of system components that must be installed prior to installing the product. Click **Install** to start the installation of missing system components (if necessary).


GFI Database Server 2.0 Setup
Welcome to the GFI Database Server 2.0 Setup Wizard
The Setup Wizard will install GFI Database Server 2.0 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
GFI
Back
Next
Cancel

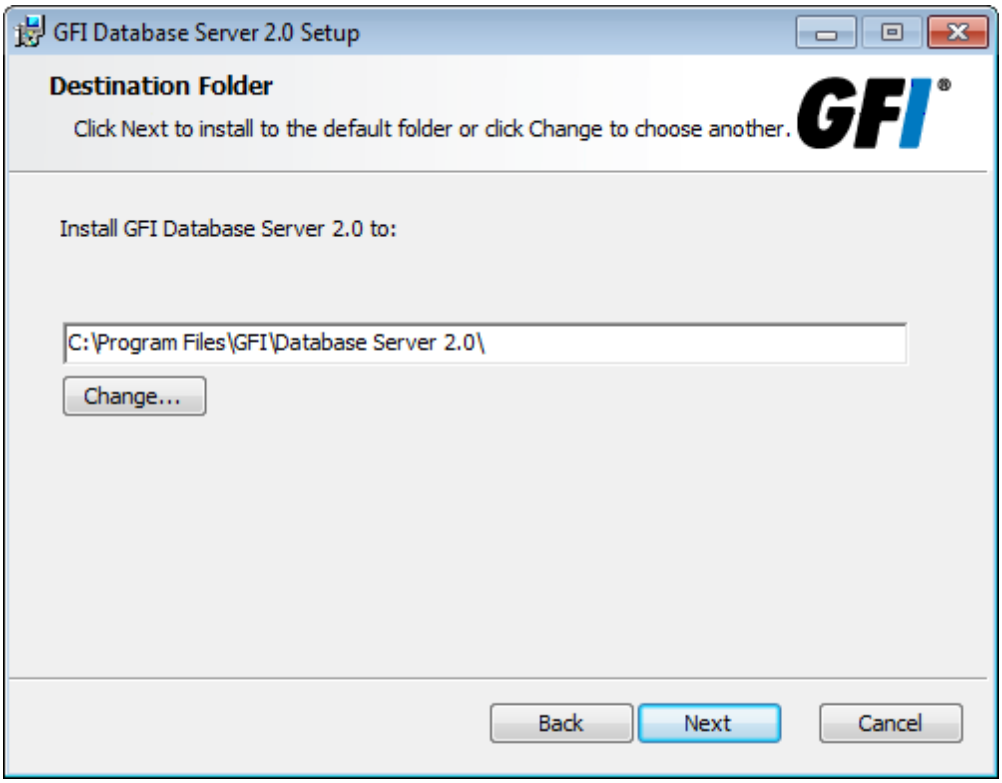
Screenshot 19: DLib Database Server

3. The DLib Database Server install wizards opens automatically after system components are installed. Click **Next** at the wizard welcome screen.

GFI Database Server 2.0 Setup
End-User License Agreement
Please read the following license agreement carefully
GFI
GFI® End-User License Agreement
For: GFI FaxMaker®; GFI MailArchiver®, GFI MailEssentials® and GFI MailSecurity®; GFI WebMonitor®; GFI LanGuard®;
GFI Network Server Monitor®; GFI EventsManager®; GFI BackUp®; GFI Device Warden™ and GFI EndPointSecurity®
("Software")
I accept the terms in the License Agreement
Print
Back
Next
Cancel

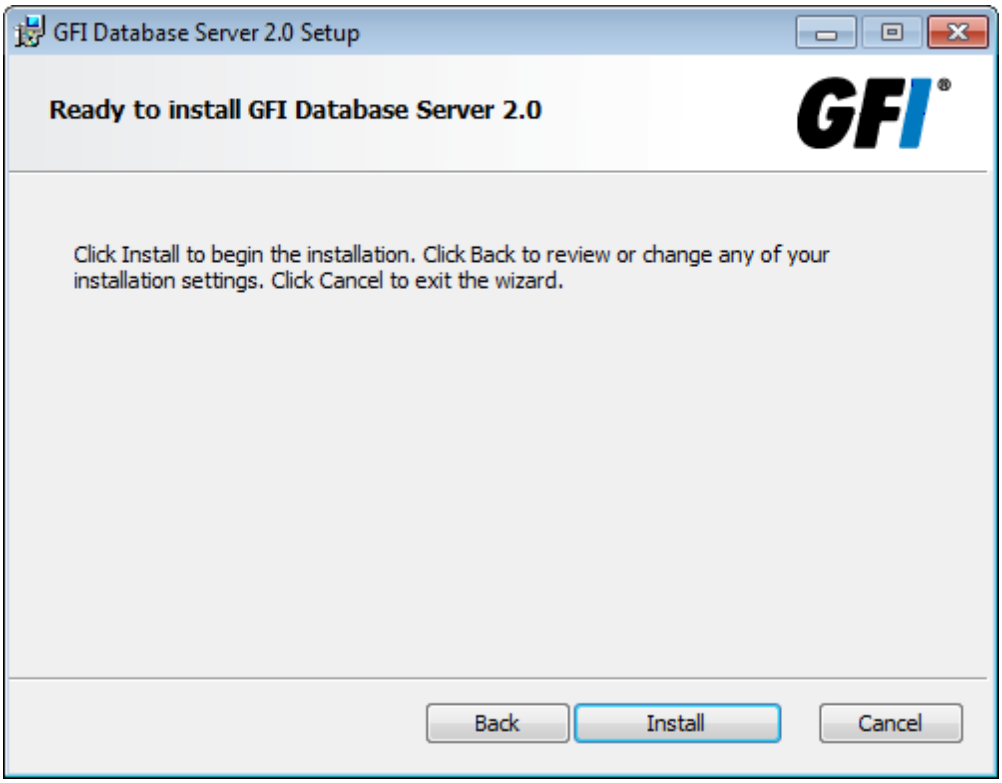
Screenshot 20: DLib Database Server EULA

4. Carefully read the license agreement. Select **I accept the terms in the License Agreement** and click **Next**.



Screenshot 21: DLib install folder

5. Click **Next** to install the database server in the default folder or click **Change...** to select an alternate folder where it is installed.

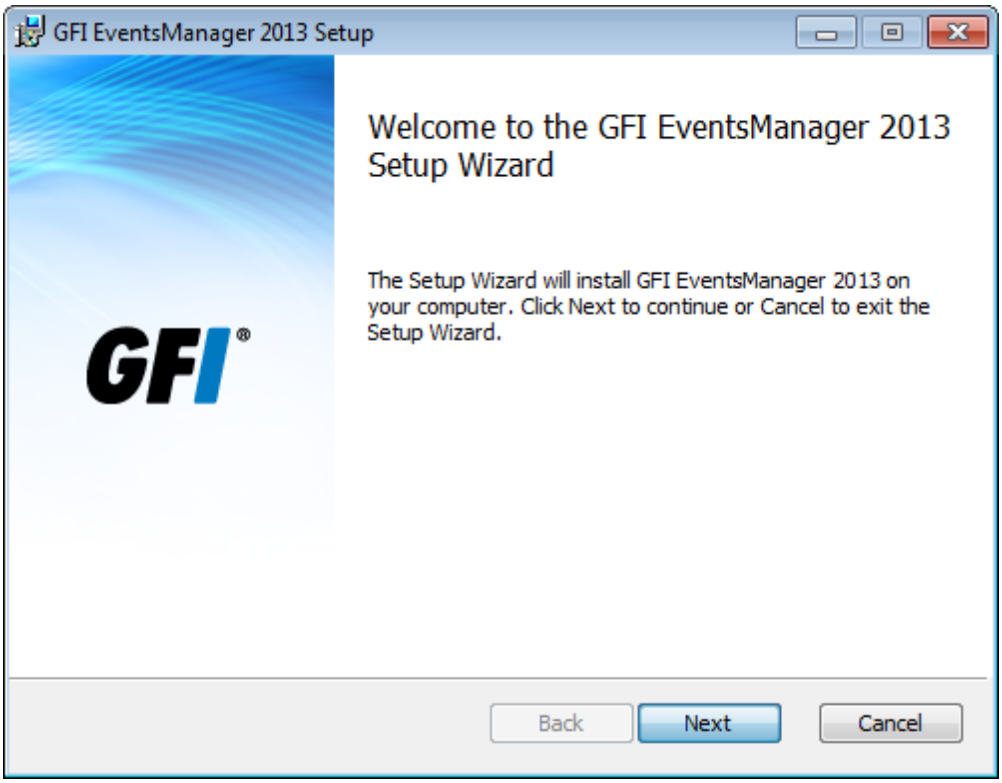

GFI Database Server 2.0 Setup
Ready to install GFI Database Server 2.0
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

Screenshot 22: Start installing DLib Database Server

6. Click **Install** to start installing DLib Database Server. Click **Finish** when prompted.

Note

After the database server is installed, the installer automatically opens the install wizard of GFI EventsManager Management Console.


GFI EventsManager 2013 Setup
Welcome to the GFI EventsManager 2013 Setup Wizard
The Setup Wizard will install GFI EventsManager 2013 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
GFI
Back
Next
Cancel

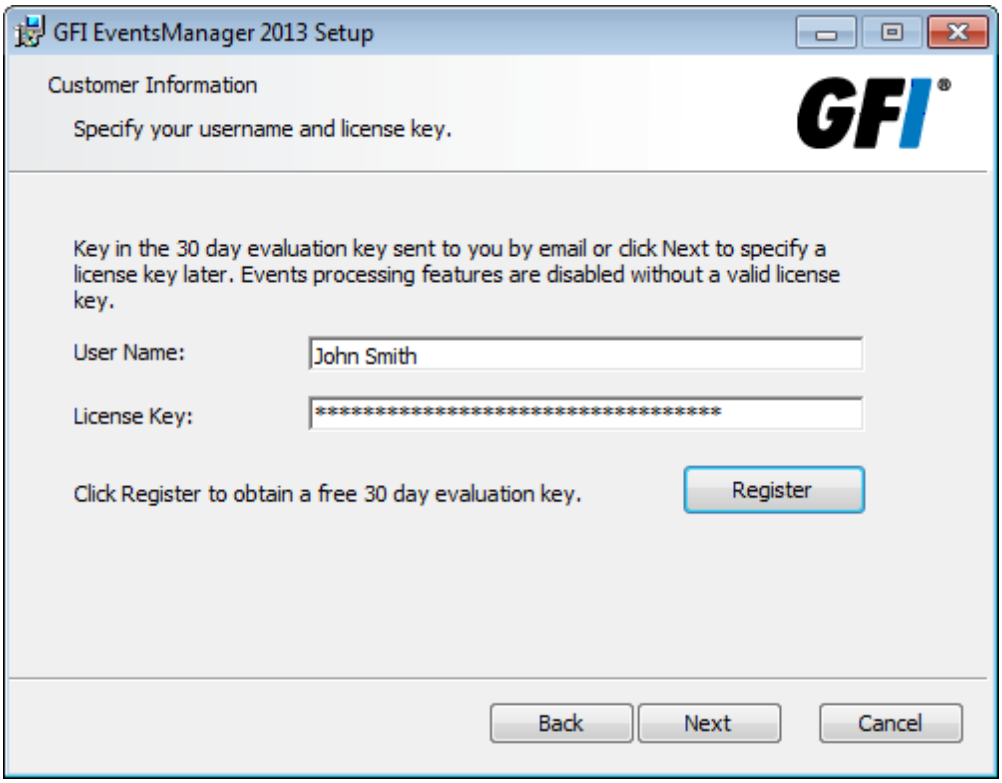
Screenshot 23: GFI EventsManager setup wizard welcome screen

7. Click **Next** at the wizard welcome screen.

GFI EventsManager 2013 Setup
End-User License Agreement
Carefully read the following end user license agreement
GFI End-User License Agreement
For: GFI FaxMaker™; GFI MailArchiver™, GFI MailEssentials™ and GFI MailSecurity™; GFI WebMonitor™; GFI LanGuard™;
GFI Network Server Monitor™; GFI EventsManager™; GFI BackUp™; GFI Device Warden™ and GFI EndPointSecurity™
("Software")
I accept the terms in the License Agreement
Print
Back
Next
Cancel

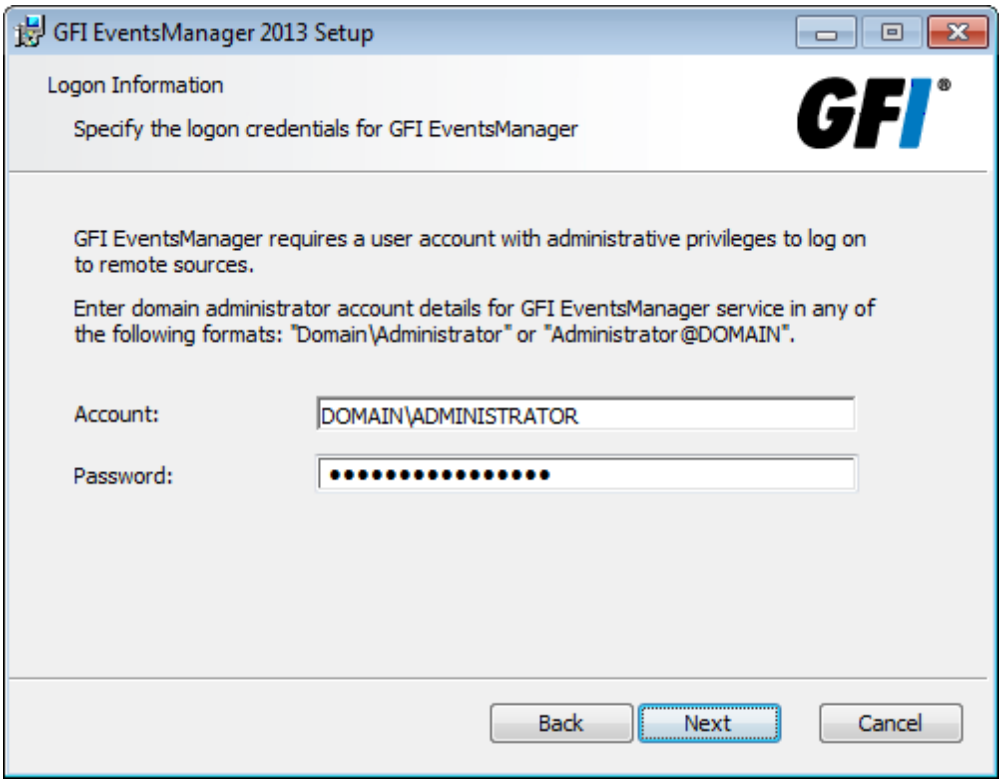
Screenshot 24: GFI EventsManager EULA

8. Carefully read the license agreement. Select **I accept the terms in the License Agreement** and click **Next**.


GFI EventsManager 2013 Setup
Customer Information
Specify your username and license key.
Key in the 30 day evaluation key sent to you by email or click Next to specify a license key later. Events processing features are disabled without a valid license key.
User Name:
John Smith
License Key:
Click Register to obtain a free 30 day evaluation key.
Register
Back
Next
Cancel

Screenshot 25: GFI EventsManager registration details

9. Key in your user name and license key in the **User Name** and **License Key** fields. To register for a free 30 day evaluation license key, click **Register**. Click **Next**.

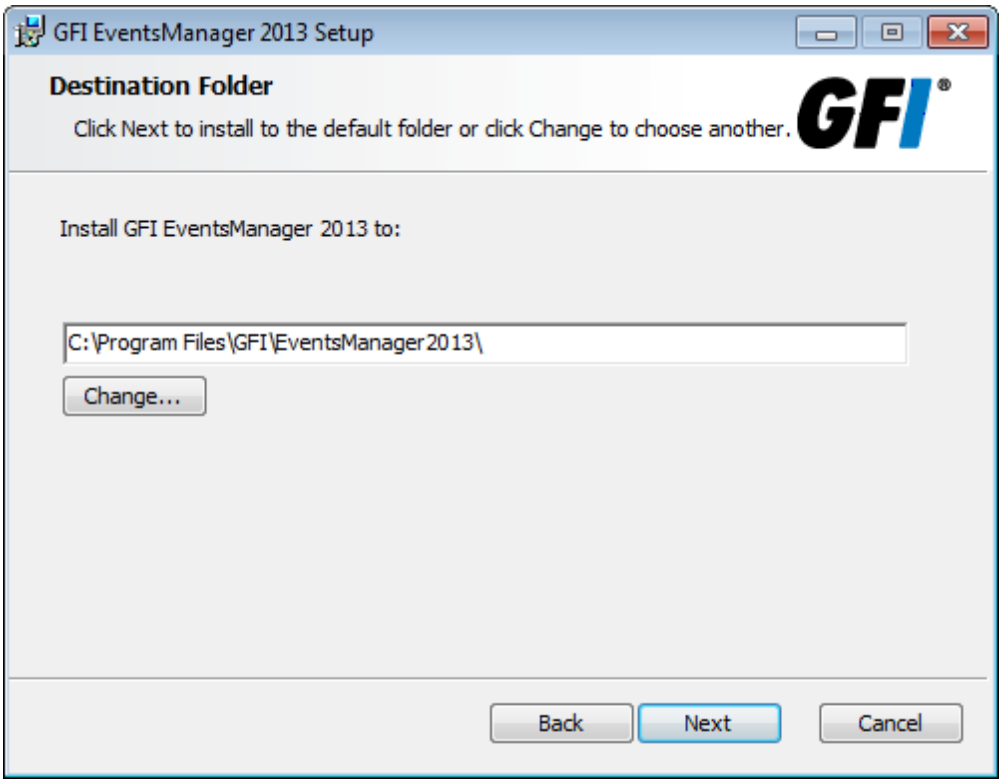

GFI EventsManager 2013 Setup
Logon Information
Specify the logon credentials for GFI EventsManager
GFI
GFI EventsManager requires a user account with administrative privileges to log on to remote sources.
Enter domain administrator account details for GFI EventsManager service in any of the following formats: "Domain\Administrator" or "Administrator@DOMAIN".
Account:
DOMAIN\ADMINISTRATOR
Password:
Back
Next
Cancel

Screenshot 26: Remote logon credentials for event log monitoring

10. Key in the logon credentials that GFI EventsManager uses to log onto remote computers.

Note

It is recommended to use a domain administrator or an account with administrative rights over all the remote computers managed by GFI EventsManager.



Screenshot 27: GFI EventsManager install folder

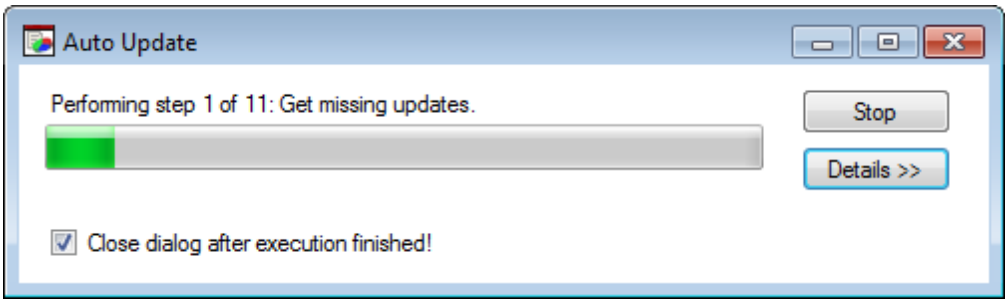
11. Click **Next** to install the Management Console in the default folder or click **Change...** to select an alternate folder where it is installed.

GFI EventsManager 2013 Setup
Ready to install GFI EventsManager 2013
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

Screenshot 28: GFI EventsManager installation completed

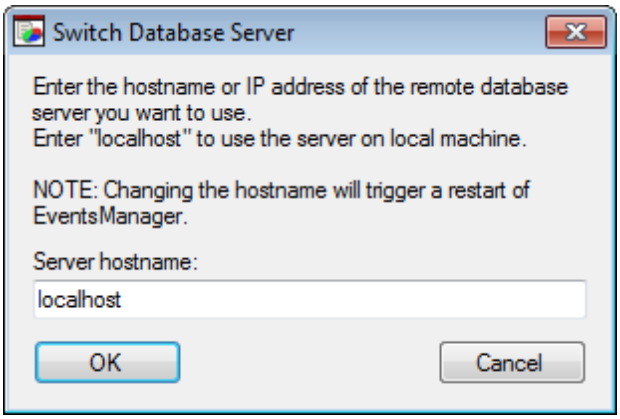
12. Click **Install** to start the installation.

13. When the installation is complete, click **Finish**.



Screenshot 29: Auto updates check

14. If GFI EventsManager detects an Internet connection, it automatically attempts to download product updates from GFI updates servers. Click **Details** to expand the information section of the Auto Update dialog and view the updates that are being downloaded.


Switch Database Server
Enter the hostname or IP address of the remote database server you want to use.
Enter "localhost" to use the server on local machine.
NOTE: Changing the hostname will trigger a restart of EventsManager.
Server hostname:
localhost
OK
Cancel

Screenshot 30: Set the database backend

> **Note**
>
> After product updates are applied, the **Switch Database Server** dialog opens. This dialog is used to link the management console to a database server. You can switch database servers from the Management Console. For more information refer to Switching between file storage databases.

15. Specify the computer that has D-Lib Database Server installed on it. If the database you want to use is on:

- A remote computer - key in the **computer name** or **IP address**
- The localhost - key in **localhost** (default).

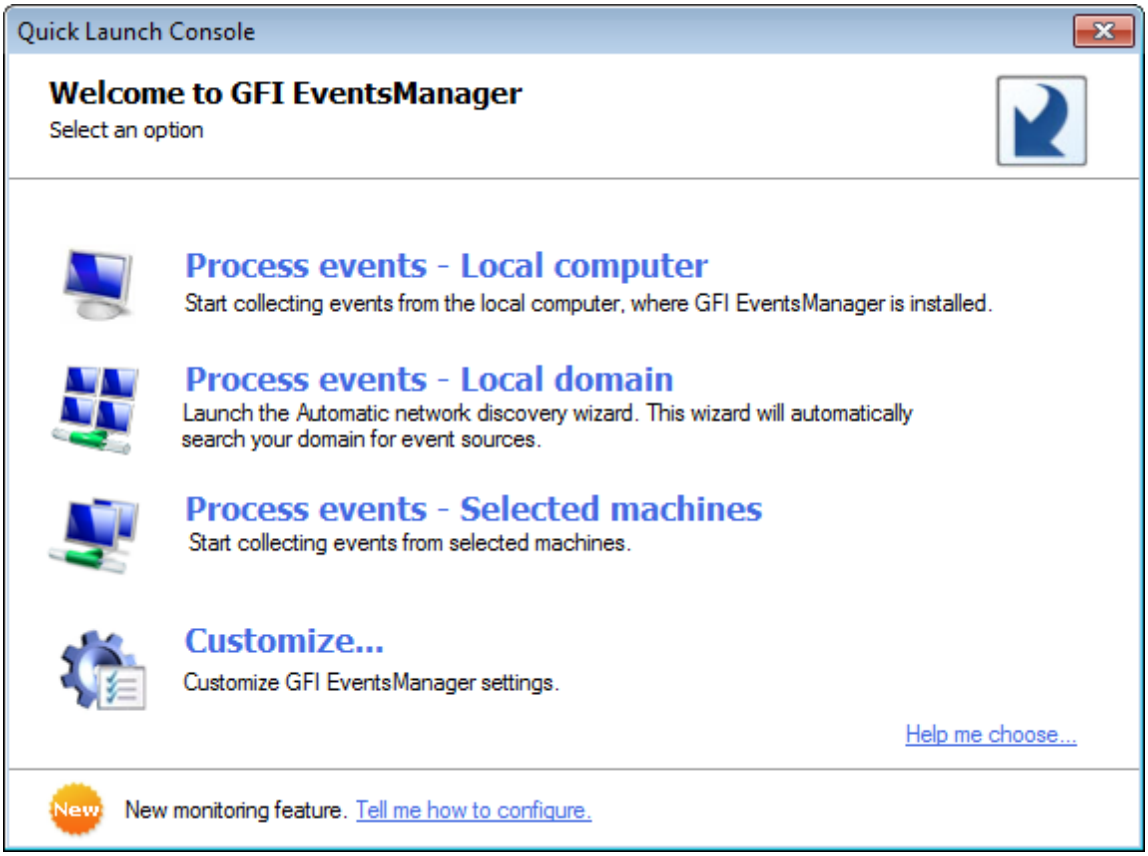
Click **OK**.

> **Note**
>
> Once the installation is complete, the Management Console opens automatically. To launch it manually, click **Start > All Programs > GFI EventsManager > Management Console**.

> **Note**
>
> Test the installation to ensure that all the components were successfully installed. For more information refer to Testing the installation.

2.5 Testing the installation

After all the required components are installed, the Management Console opens automatically. By default, it is configured to launch the **Quick Launch Console** on startup.


Quick Launch Console
Welcome to GFI EventsManager
Select an option
Process events - Local computer
Start collecting events from the local computer, where GFI EventsManager is installed.
Process events - Local domain
Launch the Automatic network discovery wizard. This wizard will automatically search your domain for event sources.
Process events - Selected machines
Start collecting events from selected machines.
Customize...
Customize GFI EventsManager settings.
Help me choose...
New
New monitoring feature. Tell me how to configure.

Screenshot 31: Running GFI EventsManager for the first time

Select an option from the Quick Launch Console to process events or customize default settings:

Table 12: Quick Launch Console options

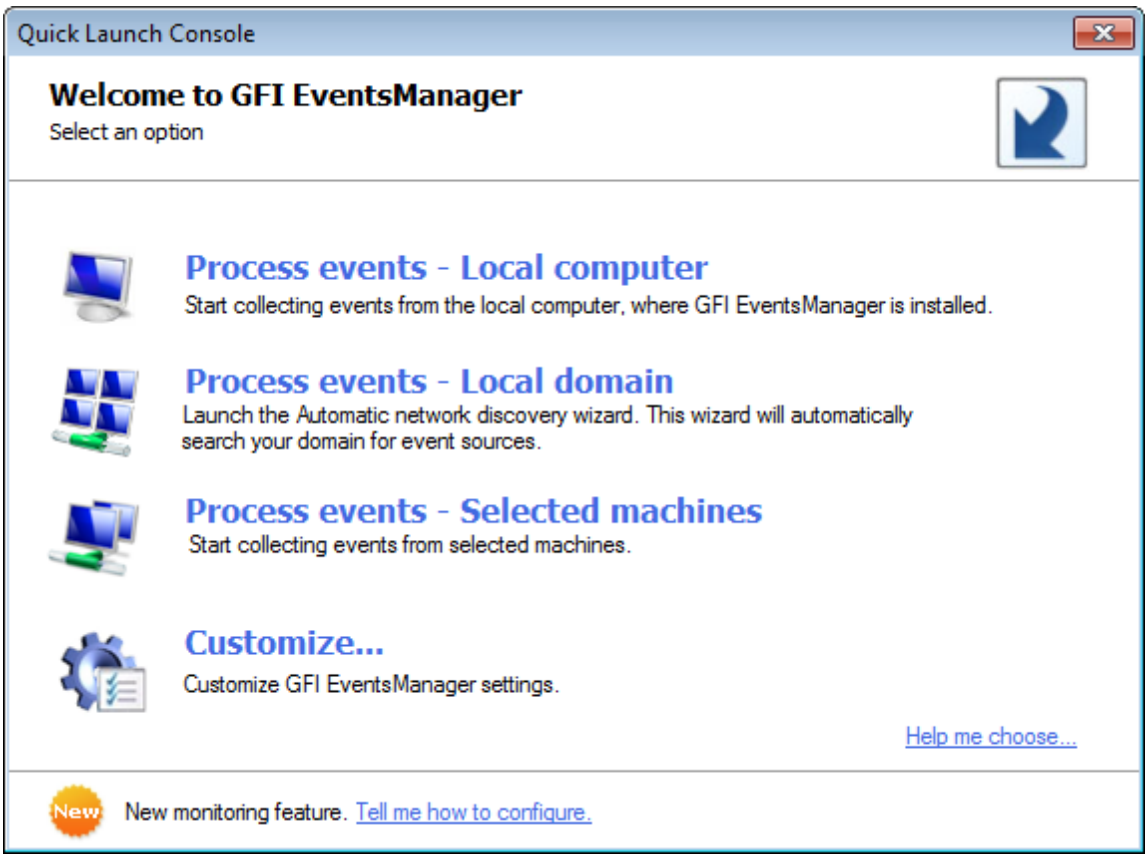
Option	Description
Process events - Local computer	Start processing logs generated by the GFI EventsManager host. **Note** For more information refer to Process events - Local computer.
Process events - Local domain	Start processing logs generated by computers and network devices within the same domain as the GFI EventsManager host. **Note** For more information refer to Process events - Local domain.
Process events - Selected machines	Start processing logs generated by specific computer(s). **Note** For more information refer to Process events - Selected machines.

Option	Description
Customize...	Customize default settings, such as: » Event sources and log types » Events processing rules » Database operations » Alert recipients » Alerting options » Active monitoring.

2.5.1 Process events - Local computer

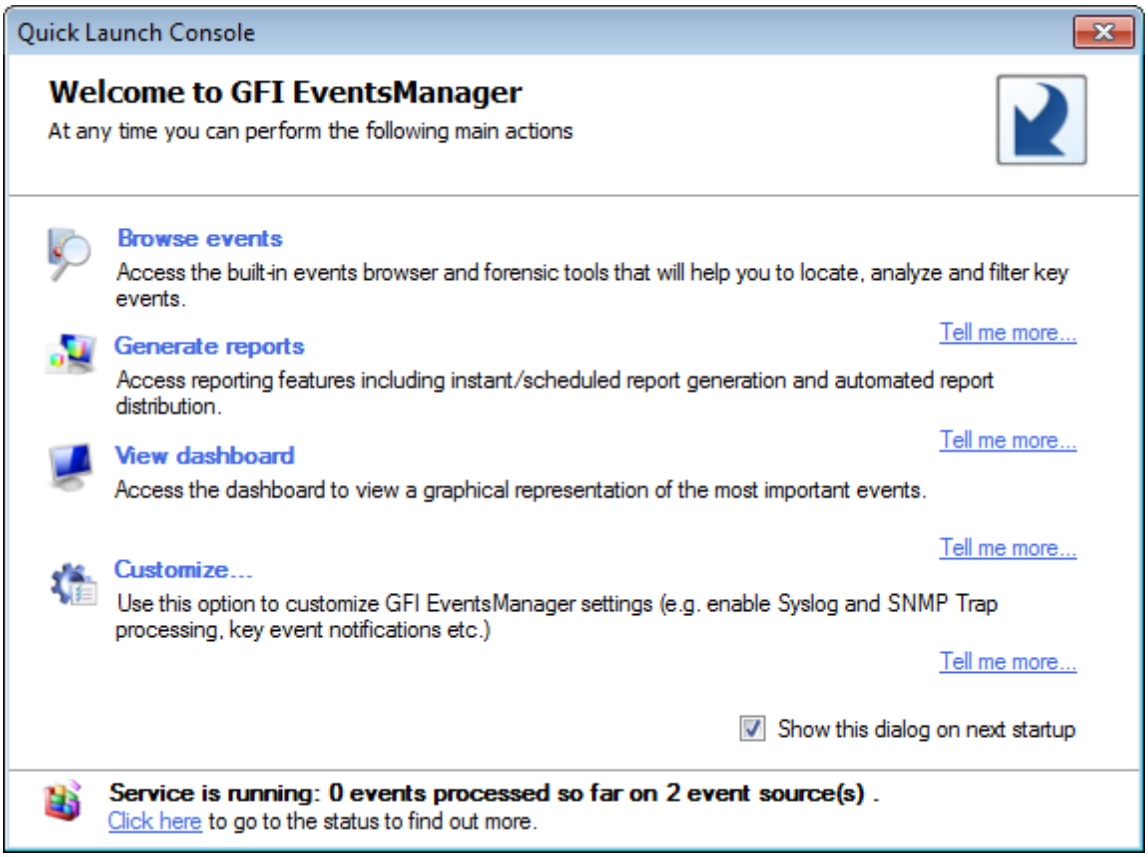
This option enables you to automatically add the localhost as an event source and start processing logs generated by it.

To process events from the local computer:


Quick Launch Console
Welcome to GFI EventsManager
Select an option
Process events - Local computer
Start collecting events from the local computer, where GFI EventsManager is installed.
Process events - Local domain
Launch the Automatic network discovery wizard. This wizard will automatically search your domain for event sources.
Process events - Selected machines
Start collecting events from selected machines.
Customize...
Customize GFI EventsManager settings.
Help me choose...
New
New monitoring feature. Tell me how to configure.

Screenshot 32: Process events - Local computer

1. Click **Process events - Local computer**.


Quick Launch Console
Welcome to GFI EventsManager
At any time you can perform the following main actions
Browse events
Access the built-in events browser and forensic tools that will help you to locate, analyze and filter key events.
Tell me more...
Generate reports
Access reporting features including instant/scheduled report generation and automated report distribution.
Tell me more...
View dashboard
Access the dashboard to view a graphical representation of the most important events.
Tell me more...
Customize...
Use this option to customize GFI EventsManager settings (e.g. enable Syslog and SNMP Trap processing, key event notifications etc.)
Tell me more...
Show this dialog on next startup
Service is running: 0 events processed so far on 2 event source(s) .
Click here to go to the status to find out more.

Screenshot 33: Console main actions

2. After the localhost logs start processing, you can:

Table 13: Quick Launch Console options

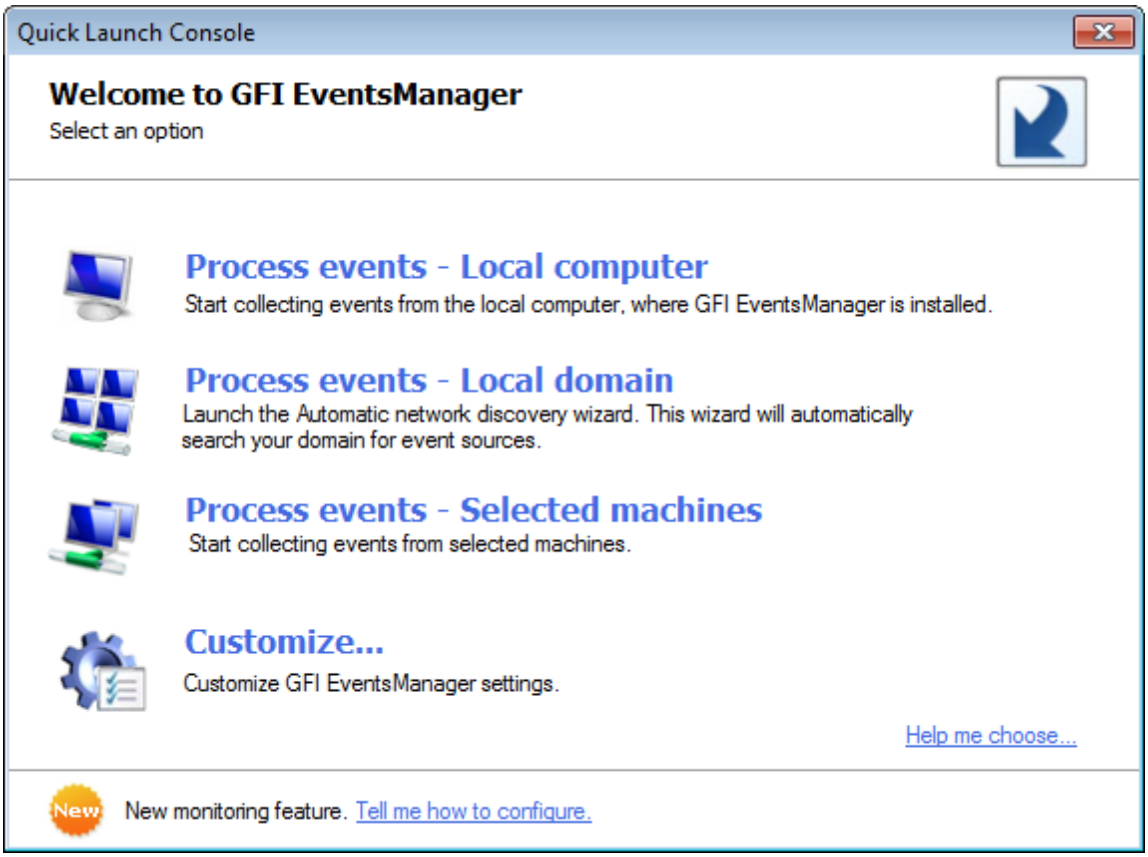
Icon	Description
	Browse events Access the built-in events and forensic tools that will help you to locate, analyze and filter key events. For more information refer to Browsing Stored Events.
	Generate reports Access reporting features including instant/scheduled report generations and automated report distribution. For more information refer to Reporting.
	View dashboard Access GFI EventsManager status dashboard. This enables you to view graphical representations of the most important events collected and processed by GFI EventsManager. For more information refer to Activity Monitoring.
	Customize Customize GFI EventsManager settings, such as enabling Syslog, SNMP Trap processing, system checks, key events notifications, and more. For more information, refer to: » Managing event sources » Configuring events processing rules » Configuring database maintenance options » Configuring alerts and default actions » Configuring Active Monitoring

> **Note**
>
> To confirm that logs are successfully processed, go to **Status** tab > **Job Activity** and check that there are activity logs under the **Operational History** section.

2.5.2 Process events - Local domain

This option enables you add one or more computers that are on the same domain or workgroup as GFI EventsManager. The Automatic Network Discovery wizard enables you to select the type of event sources you want to add and then lists the sources that are detected.

To process event from computers on the same domain/workgroup:


Quick Launch Console
Welcome to GFI EventsManager
Select an option
Process events - Local computer
Start collecting events from the local computer, where GFI EventsManager is installed.
Process events - Local domain
Launch the Automatic network discovery wizard. This wizard will automatically search your domain for event sources.
Process events - Selected machines
Start collecting events from selected machines.
Customize...
Customize GFI EventsManager settings.
Help me choose...
New
New monitoring feature. Tell me how to configure.

Screenshot 34: Process events - Local domain

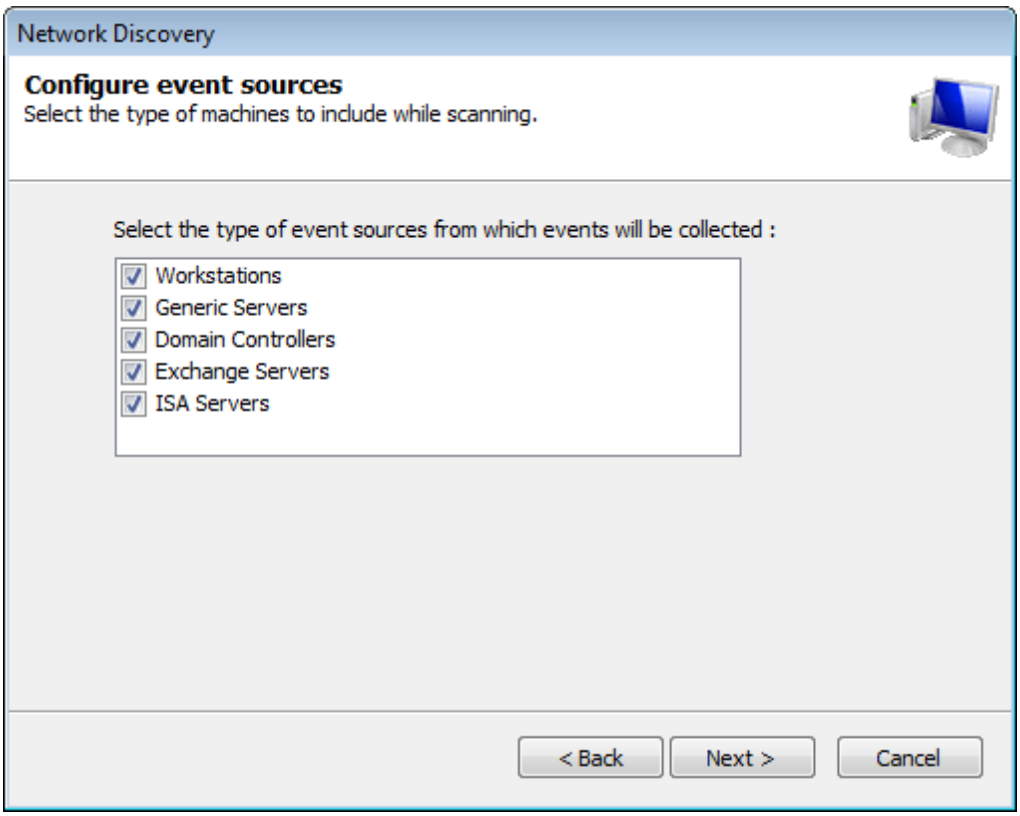
1. Click **Process events - Local domain**. This opens the **Automatic Network Discovery** wizard.

> **Note**
>
> The wizard can also be launched from **Configuration** tab > **Event Sources**. From the left pane, right-click **All event sources** and select **Scan local domain**.

Network Discovery
Welcome to the Automatic network discovery wizard
This wizard searches the entire network for computers and servers.
Stage 1: Configure the event sources to include when scanning the local domain.
Stage 2: Search network for target computers. The wizard will collect information from all network computers using credentials used by the EventsManager Service.
Stage 3: Select network computers. Selected computers will be added as event sources.
Finish
< Back
Next >
Cancel

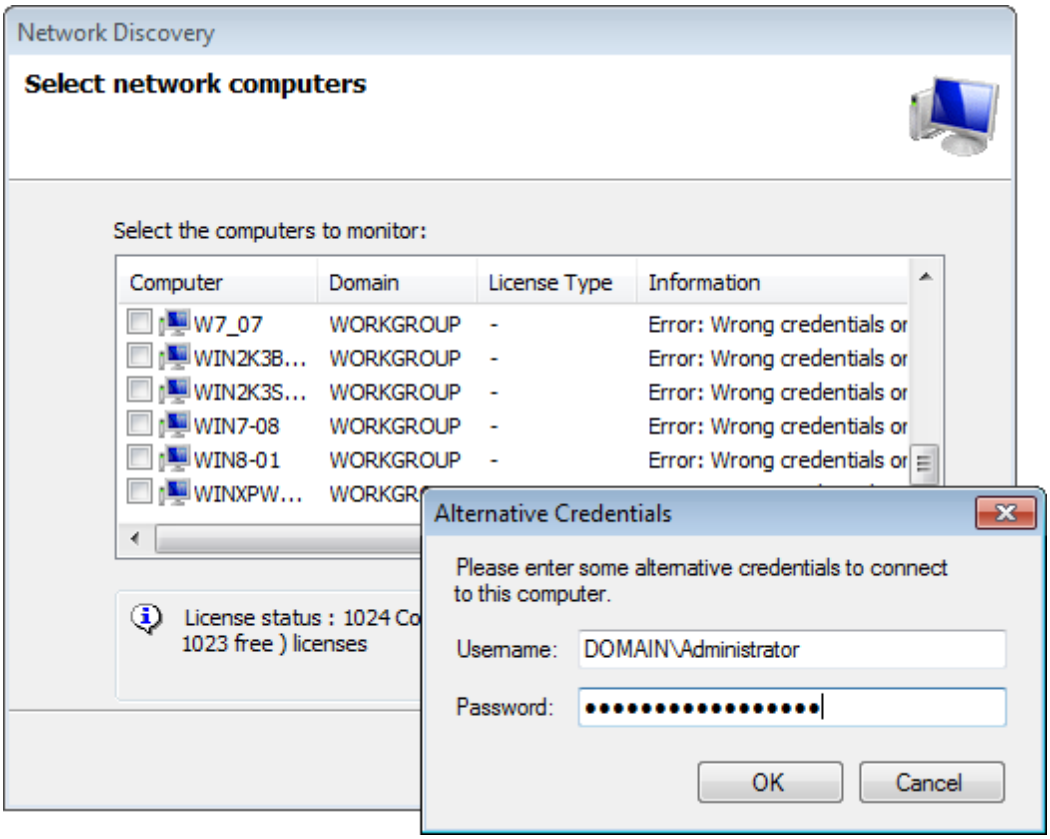
Screenshot 35: Automatic discovery wizard

2. Click **Next** at the wizard welcome screen.



Screenshot 36: Select event source types to detect on your network

3. Select the type of event sources that the wizard will attempt to detect on your network. Click **Next**.



Screenshot 37: Search network progress

Note

If GFI EventsManager detects computers that cannot be logged onto using the supplied credentials, it enables you to specify alternate logon credentials for each computer you select.

4. Select a computer from the list and key in the username and password. Click **OK** to close the **Alternative Credentials** dialog.

Note

Repeat this step until all the required sources are added.

5. Click **Next** and **Finish**.

Note

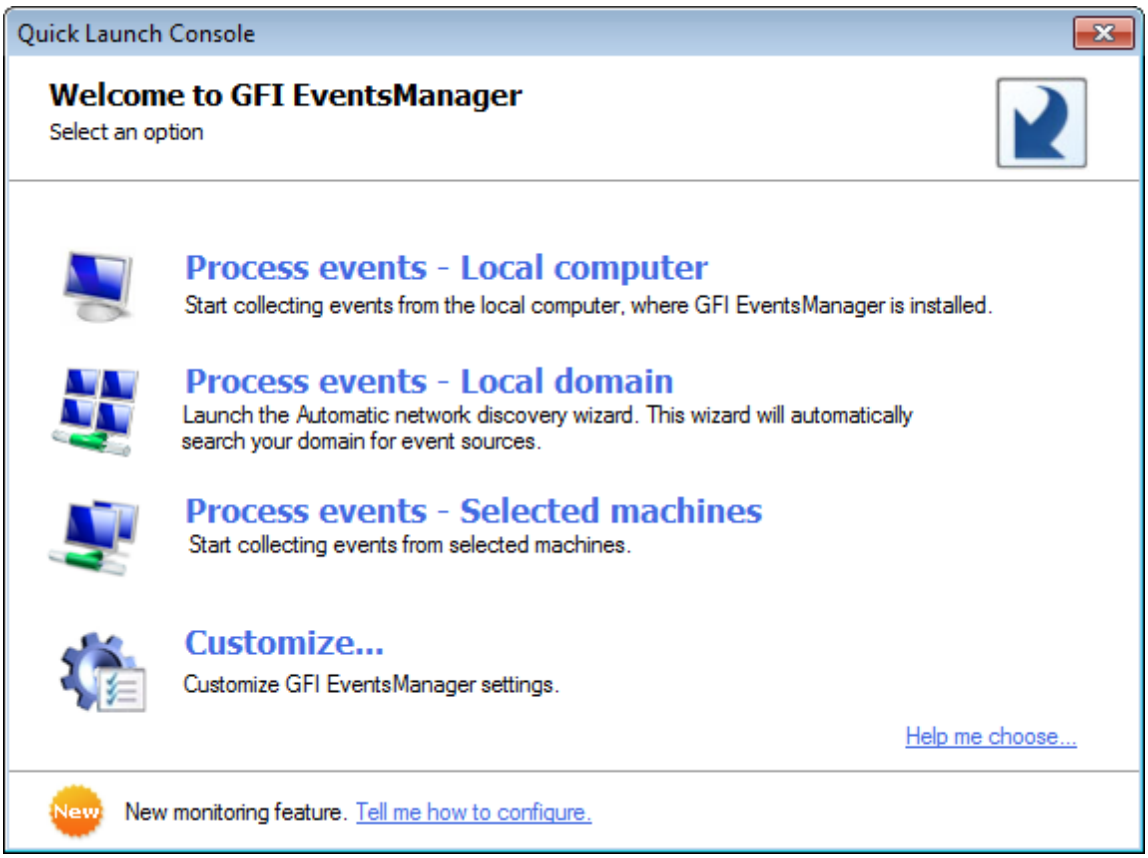
To automatically add new computers that are joined to the same domain/workgroup as GFI EventsManager, you must configure Synchronization Options. For more information refer to Adding event sources automatically.

2.5.3 Process events - Selected machines

This option enables you to add specific computers manually, by:

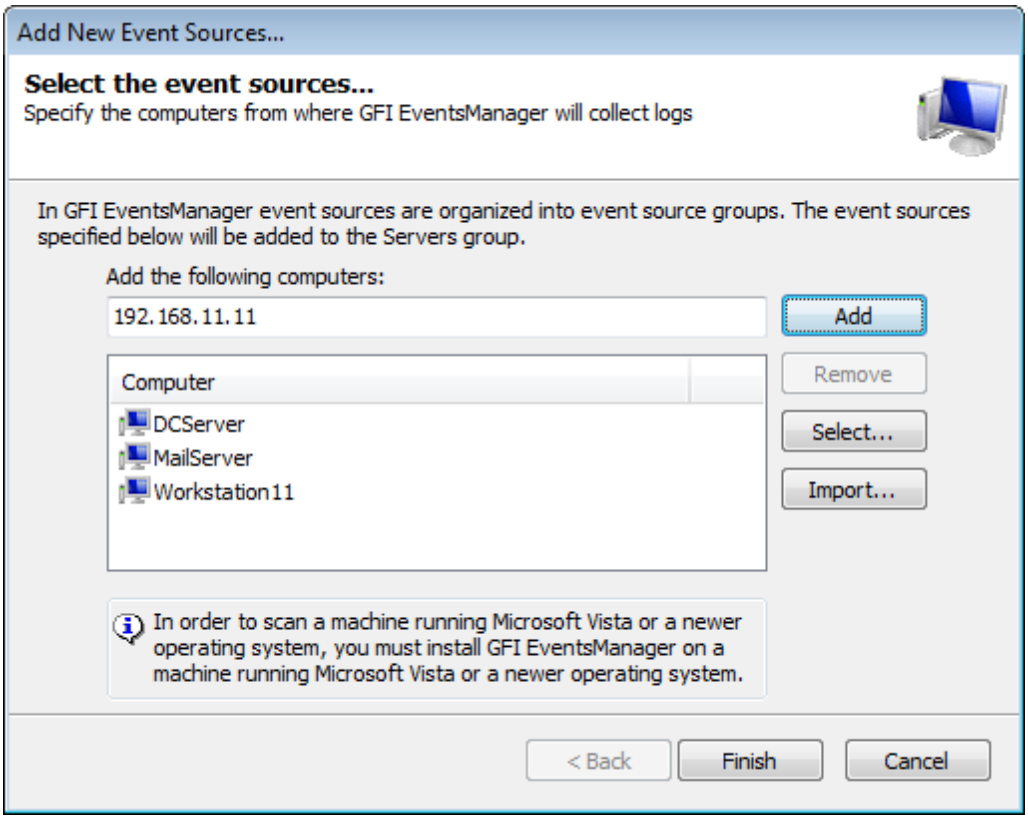
- Keying in computer names and IPs
- Selecting computers from reachable domains and workgroups
- Importing computers from a text file containing a single computer name per line.

To process events of selected machines:


Quick Launch Console
Welcome to GFI EventsManager
Select an option
Process events - Local computer
Start collecting events from the local computer, where GFI EventsManager is installed.
Process events - Local domain
Launch the Automatic network discovery wizard. This wizard will automatically search your domain for event sources.
Process events - Selected machines
Start collecting events from selected machines.
Customize...
Customize GFI EventsManager settings.
Help me choose...
New
New monitoring feature. Tell me how to configure.

Screenshot 38: Process events - Selected machines

1. Click **Process events - Selected machines.**
2. This opens the **Add New Event Source** dialog.


Add New Event Sources...
Select the event sources...
Specify the computers from where GFI EventsManager will collect logs
In GFI EventsManager event sources are organized into event source groups. The event sources specified below will be added to the Servers group.
Add the following computers:
192.168.11.11
Add
Computer
DCServer
MailServer
Workstation11
Remove
Select...
Import...
In order to scan a machine running Microsoft Vista or a newer operating system, you must install GFI EventsManager on a machine running Microsoft Vista or a newer operating system.
< Back
Finish
Cancel

Screenshot 39: Add new event source wizard

3. The following table describes the available options:

Table 14: Adding new event sources manually

Option	Description
Add	Key in the computer name or IP address in the **Add the following computers** field. Click **Add** to add the specified computer to the **Computer** list. **Note** Repeat this step until you add all the event sources to the selected group. **Note** Since Syslog and SNMP traps use IP addresses to determine the source of an event, it is recommended to use the source IP address instead of the computer name when adding Syslog and SNMP Traps sources.
Remove	Select one or more computers from the **Computer** list and click **Remove** to delete them from the list.
Select...	Click **Select...** to launch the **Select Computers...** dialog: 1. From the **Domain** drop-down menu, select the domain you want to scan for available sources and click **Search**. 2. From the search results list, select the computers you want to add. 3. Click **OK** to close the **Select Computers...** dialog and return to the **Add New Event Sources...** dialog.
Import...	Click **Import...** to import computers from a text file. Ensure that the text file contains only one computer name or IP address per line.

4. Click **Finish** to finalize your settings. GFI EventsManager immediately attempts to scan the added event sources, using the default logon credentials. For more information refer to Configuring event source logon credentials.

Note

If synchronization is not enabled, you can use the **Network Discovery Wizard** to automatically search and add events sources. To launch **Network Discovery Wizard**, right-click **All event sources** from the event sources tree and select **Scan local domain**. For more information refer to Adding event sources automatically.

Note

To confirm that logs are successfully processed, go to **Status** tab **> Job Activity** and check that there are activity logs under the **Operational History** section.

3 Achieving Results

This chapter provides information on how to use GFI EventsManager to achieve results. The information provided helps you conduct positive forensic investigations and system monitoring. It also enables you to achieve positive legal compliance results, while ensuring network security at all times.

Topics in this chapter:

3.1 Achieving Network Security 62

3.2 Effective System Health Monitoring 64

3.3 Achieving PCI DSS Compliance 66

3.1 Achieving Network Security

Many companies mistakenly assume that unauthorized access is an external threat only. The majority of corporate security threats actually stem from internal sources, against which a firewall offers no protection. A good security strategy includes real-time monitoring for critical security events and periodic analysis of your systems' security logs so that you can detect and respond quickly to attacks.

Network security is defined as a set of rules and policies adopted by a network administrator to monitor and prevent misuse and unauthorized access of a network. For an effective secure network strategy follow the steps described below:

1. Add Management Console Users and Groups

GFI EventsManager can be managed by multiple users. You can link console activity to different users by creating a user for each person who is accessing the console and making changes to configurations.

- Create users to be able to audit individual activity. For more information refer to Managing user accounts.
- Create user groups so that multiple users can be managed at once. For more information refer to Managing user groups.

2. Configure console security options

GFI EventsManager enables you to configure console security options to facilitate securing sensitive information.

- Enable GFI EventsManager login system so that users can be tracked individually. For more information refer to Enabling the login system.
- Configure anonymization options so that unauthorized users are not able to view sensitive information within the management console. For more information refer to Anonymization.
- Enable user auditing so that an activity log can be created for each user who changes system configurations. For more information refer to Auditing console activity.

3. Configure Alerts and Default Actions

GFI EventsManager enables you to keep track of network activity in real-time by triggering alerts, execute scripts and perform other operations when certain event logs are collected.

- Configure alert recipients and notification settings for SMS, Email, Network and SNMP messages. For more information refer to Configuring Alerting Options.
- Configure operations that are performed on detection of specific attributes of an event log. For more information refer to Configuring Default Classification Actions.

---

4. Add event sources

If you haven't done already, add the event sources that you want to secure.

- Add event sources manually by specifying IP addresses and/or computer names. For more information refer to Adding event sources manually.
- Add event sources automatically, as soon as they are joined to the domain or network. For more information refer to Adding event sources automatically.

---

5. Enable event source auditing permissions

In order to audit event sources, Auditing options must be enabled from the source operating system.

- Manually enable auditing options for single computers. For more information refer to Enabling event source permissions manually.
- Automatically enable auditing options for larger groups of computers. For more information refer to Enabling event source permissions automatically.

---

6. Collect event logs

Start collecting event logs generated by the sources added in the previous step. Event logs can be collected as soon as the source is added, however, you can further customize event source settings to retrieve specific information.

- Configure event source properties such as logon credentials, licensing type and more. For more information refer to Configuring event source properties.
- Configure event sources to collect and process Windows Event Logs, SNMP Traps Messages, Text Logs and more. For more information refer to Collecting Event Logs.

---

7. Analyze the collected event logs and monitor activity

After collecting the required event logs, you are able to analyze them from Events Browser. Events Browser allows you to create custom rules from the collected logs. This enables you to trigger alerts or actions when events of the same type are collected.

- Create rules based on collected events. Events processing rules check an event log and perform actions based on the settings configured in Step 3. For more information refer to Creating new rules from existing events.
- Monitor events management activity from the extensive dashboard views. For more information refer to Activity Monitoring.

3.2 Effective System Health Monitoring

GFI EventsManager is able to perform thorough system checks on your servers and workstations. It uses Active Monitoring to help you detect and proactively fix system errors and hardware defects, to prevent network disasters.

System checks are able to monitor mission-critical servers including Microsoft® ISA Server®, Exchange Server®, SQL Server® and IIS®. They can even be configured to delve deeper into systems and monitor email queues, SMTP gateways, MAPI availability, bad hard disk blocks, disk space, and more.

Monitoring the effectiveness of rules and policies enforced on your systems helps determine how well plans and actions are working in practice.

---

1. Add event sources

After GFI EventsManager is installed, it automatically adds the localhost to the list of event sources. Add other sources manually or automatically, according to your preferences.

- Add computers manually by specifying computer names, IP addresses. For more information refer to Adding event sources manually.
- Computers can also be added automatically as soon as they are discovered by GFI EventsManager. For more information refer to Adding event sources automatically.

---

2. Configure event sources

Configure event source properties to enable active monitoring and events processing. Refer to the following sections for information about:

- Configuring event source properties
- Configuring event source monitoring
- Collecting event logs.

---

3. Configure alerts and default actions

One of the key features of GFI EventsManager is the ability to send notifications and perform pre-defined actions when certain event logs are collected.

Plan how notifications are sent and configure mail server, SMS gateway or network settings accordingly. Add recipients in GFI EventsManager to which notifications are sent.

Once complete, configure the default actions to perform when specific events are processed. Refer to the following section for information about:

- Configuring the administrator account
- Managing user accounts
- Configuring alerting options
- Configuring default classification actions.

---

4. Configure Active Monitoring

Active Monitoring Checks are conditional parameters, run against event sources on based a schedule. Whether the parameter conditions are being met or not, monitoring checks generate event logs.

The generated event log can be combined with events processing rules to further analyze the issue that generated the log, send notifications, execute scripts and perform remedial actions.

GFI EventsManager contains a few generic Active Monitoring that you can use out of the box. You can also create new ones and configure granular settings to acquire accurate and meaningful information. Refer to the following sections for information about:

- Active Monitoring
- Creating and configuring root folders
- Creating and configuring Active Monitoring
- Applying Active Monitoring
- Analyzing Active Monitoring activity.

---

5. Configure events processing rules

Events processing rules are conditional checks that are run against collected event logs. Based on the information found in the event log (such as **Log Type**, **Timestamp** and **Classification**) GFI EventsManager determines the action that has to be performed.

Create new rules from event logs generated by active monitoring checks to trigger automatic remedial operations when a system error is detected.

Optionally, configure event sources to run System Health rules against collected event logs. Refer to the following sections for information about:

- Events processing rules
- About events processing rules
- Managing rules-set folders
- Creating new rules from existing events
- Configuring rule conditions
- Configuring event sources to process logs with System Health rules.

---

6. Generate reports

GFI EventsManager enables you to generate reports for technical IT staff as well as executive summary reports for management personnel. Reports help you visualize your network information, through graphs and charts, as well as statistical information provided in your reports.

GFI EndPointSecurity ships with variety of pre-defined reports and also allows you to create new reports or modify existing ones.

- Available reports
- Generating reports
- Managing Reports
- Creating custom reports
- Configuring report filtering conditions.

3.3 Achieving PCI DSS Compliance

The Payment Card Industry (PCI) Data Security Standard (DSS) is a standard defining a list of requirements for security management, policies, network architecture and other measures that helps protect a customer's account and credit card information details.

Full compliance with PCI DSS requires complete event log management coupled with extensive reporting, GFI EventsManager is therefore an essential solution to assist with your PCI compliance program. To learn more about how to be compliant with PCI DSS, use the following links:

Whitepaper on PCI DSS Compliance and GFI Software Products

Review GFI white papers on PCI DSS Compliance:

- http://go.gfi.com/?pageid=EM_PCIDSS

How GFI EventsManagercan assist in PCI DSS compliance

- Regularly monitor events management activities. For more information refer to Activity Monitoring.
- Apply event processing rules based on PCI DSS requirements list. For more information refer to Events Processing Rules.
- Generate reports regularly to monitor events. For more information refer to Reporting.

4 Managing Event Sources

This chapter provides you with information about adding and managing your event sources. Event sources are networked computers and devices that are accessed and processed by GFI EventsManager. The Events Sources sub-tab, enables you to organize your event sources into specific groups. You can create new groups or use the default ones to distinctively configure and organize event sources.

Topics in this chapter:

4.1 Adding event sources manually 67

4.2 Adding event sources automatically 68

4.3 Creating a new event source group 71

4.4 Configuring event source properties 73

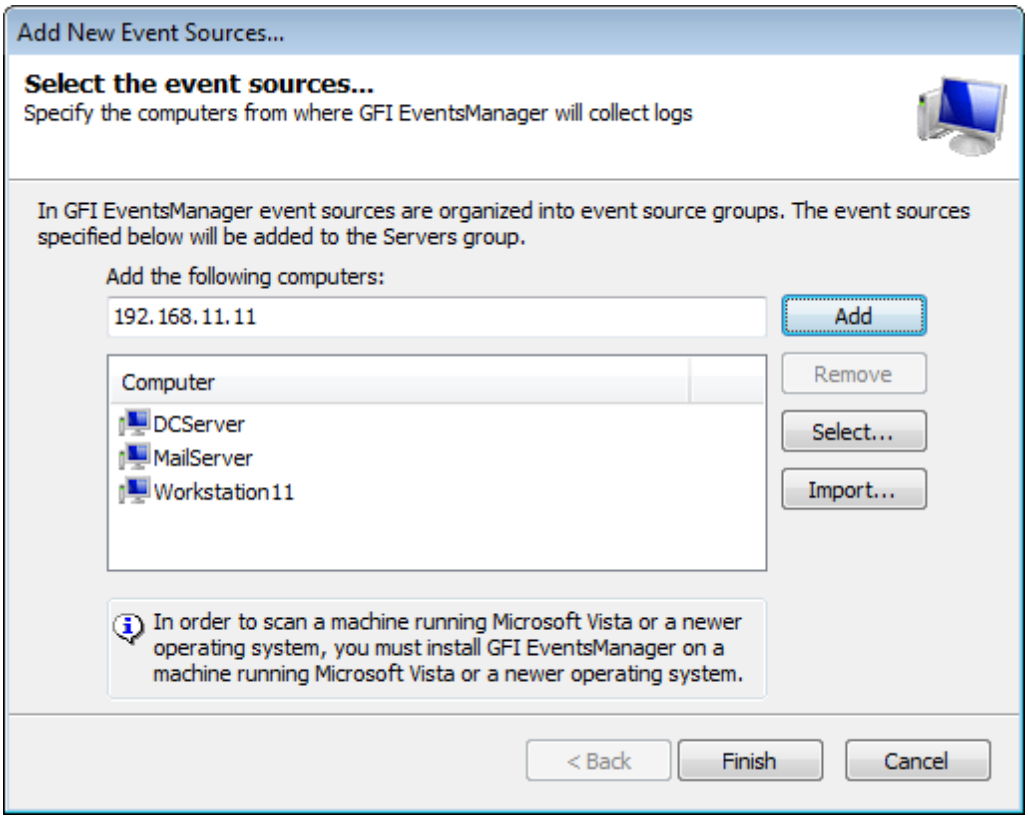
4.5 Database sources 81

4.1 Adding event sources manually

To manually add a new event sources to a computer group:

1. Click **Configuration** tab > **Event Sources** and from **Group Type**, select **Event Sources Groups**.

2. Right-click a computer group of your choice and select **Add new event source...**


Add New Event Sources...
Select the event sources...
Specify the computers from where GFI EventsManager will collect logs
In GFI EventsManager event sources are organized into event source groups. The event sources specified below will be added to the Servers group.
Add the following computers:
192.168.11.11
Add
Remove
Select...
Import...
Computer
DCServer
MailServer
Workstation11
In order to scan a machine running Microsoft Vista or a newer operating system, you must install GFI EventsManager on a machine running Microsoft Vista or a newer operating system.
< Back
Finish
Cancel

Screenshot 40: Add new event source wizard

3. The following table describes the available options:

Table 15: Adding new event sources manually

Option	Description
Add	Key in the computer name or IP address in the **Add the following computers** field. Click **Add** to add the specified computer to the **Computer** list. **Note** Repeat this step until you add all the event sources to the selected group. **Note** Since Syslog and SNMP traps use IP addresses to determine the source of an event, it is recommended to use the source IP address instead of the computer name when adding Syslog and SNMP Traps sources.
Remove	Select one or more computers from the **Computer** list and click **Remove** to delete them from the list.
Select...	Click **Select...** to launch the **Select Computers...** dialog: 1. From the **Domain** drop-down menu, select the domain you want to scan for available sources and click **Search**. 2. From the search results list, select the computers you want to add. 3. Click **OK** to close the **Select Computers...** dialog and return to the **Add New Event Sources...** dialog.
Import...	Click **Import...** to import computers from a text file. Ensure that the text file contains only one computer name or IP address per line.

4. Click **Finish** to finalize your settings. GFI EventsManager immediately attempts to scan the added event sources, using the default logon credentials. For more information refer to Configuring event source logon credentials.

Note

If synchronization is not enabled, you can use the **Network Discovery Wizard** to automatically search and add events sources. To launch **Network Discovery Wizard**, right-click **All event sources** from the event sources tree and select **Scan local domain**. For more information refer to Adding event sources automatically.

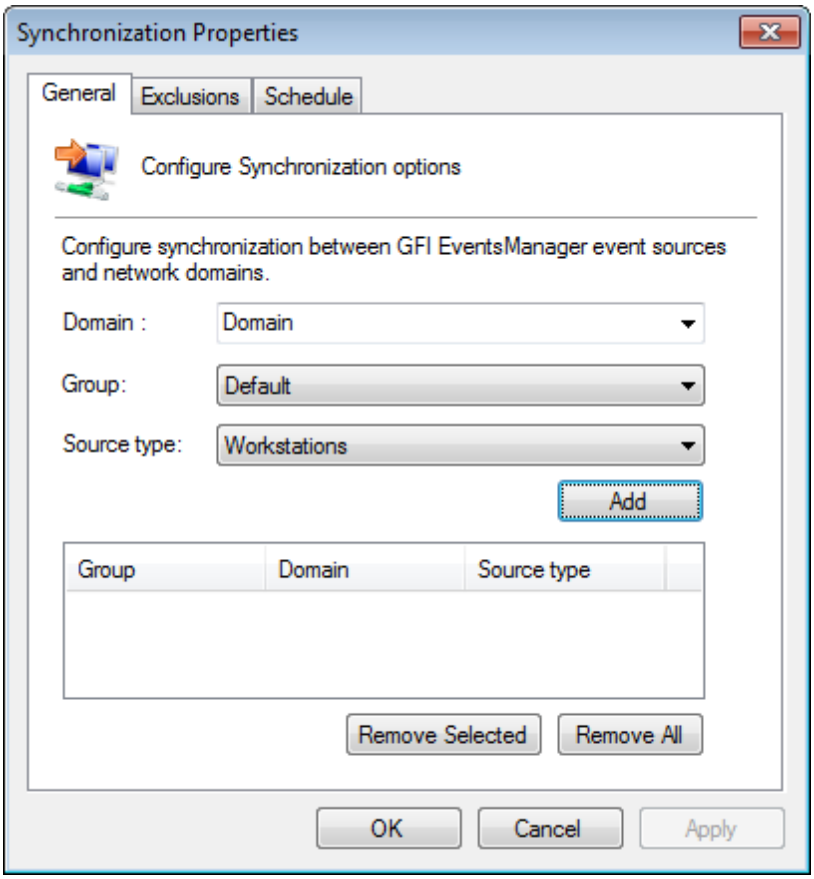
4.2 Adding event sources automatically

GFI EventsManager enables you to automatically synchronize domains with event sources groups. When synchronization is configured, every new domain member is automatically added to GFI EventsManager's event source list.

To enable auto synchronization:

1. Click **Configuration** tab > **Event Sources** and from **Group Type**, select **Event Sources Groups**.

2. Right-click **All event sources** and select **Edit synchronization options**.



Screenshot 41: Synchronization properties - General tab

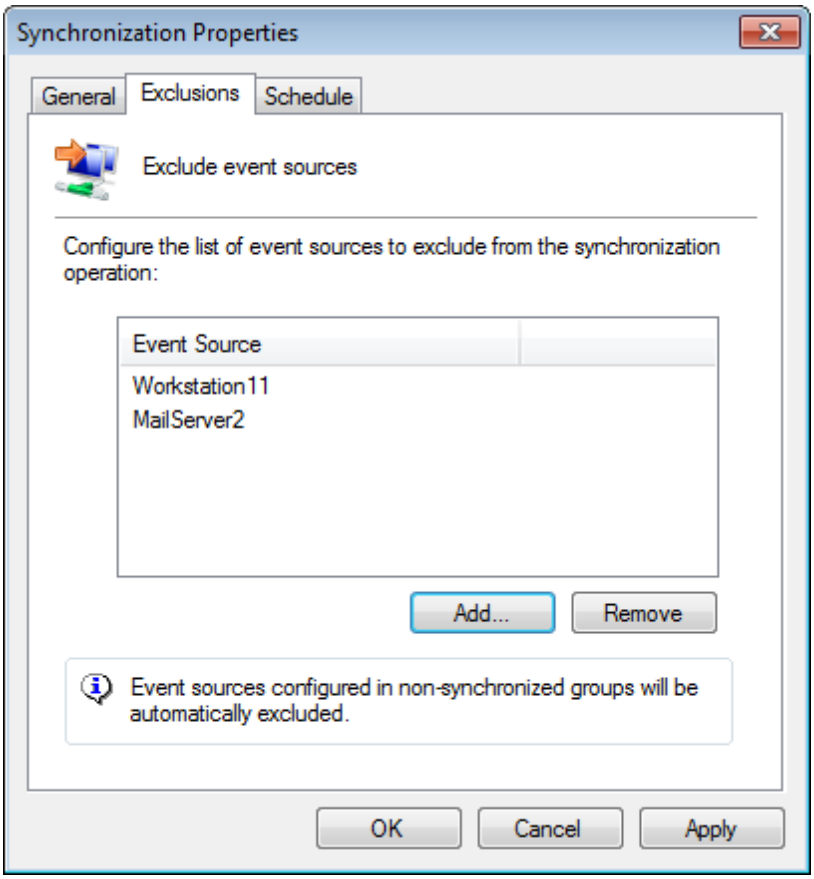
3. Select **General** tab and configure the options described below:

Table 16: Synchronization properties - General tab

Option	Description
Domain	Select the domain name from the list or key in a valid domain name.
Group	Select the GFI EventsManager group name where to add the discovered event sources.
Source type	Select the type of event sources that GFI EventsManager scans for, in the specified domain.

4. To include the synchronization click **Add**.

5. Repeat steps 3 to 4 for each domain you want to synchronize.

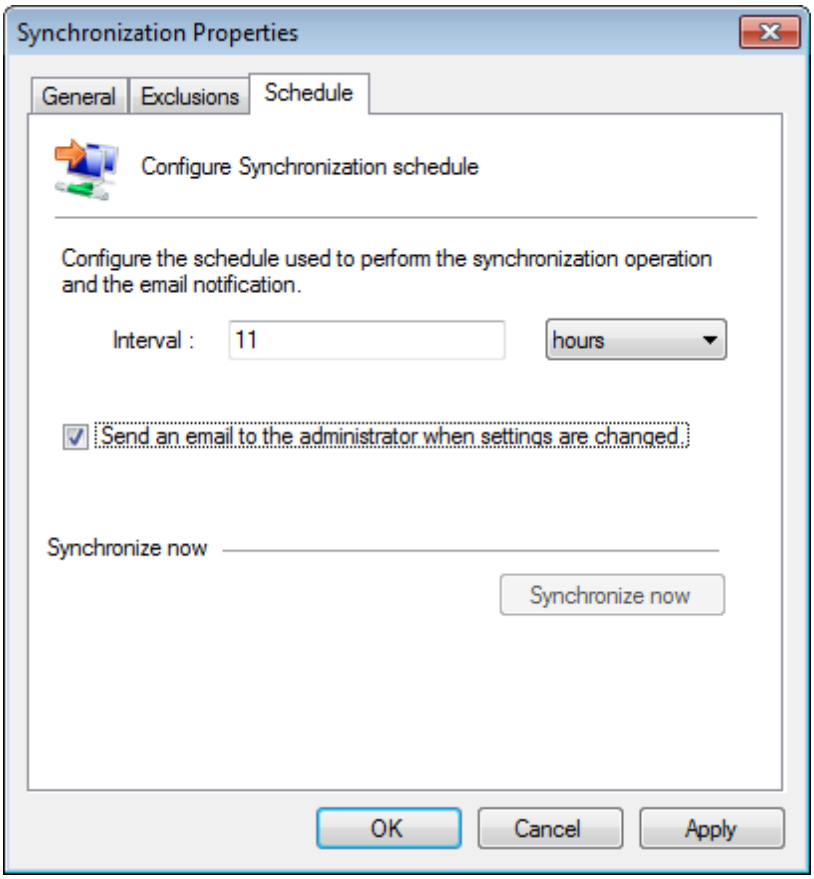


Screenshot 42: Excluding computers from automatic synchronization

6. (Optional) Select **Exclusions** tab to configure the list of computers that will be excluded from synchronization. Click **Add** and key in a computer name to exclude.

> **Note**
>
> Event sources that are already part of an event source group will be automatically excluded from synchronization.

7. Select **Schedule** tab to configure when the synchronization should be performed.



Screenshot 43: Synchronization properties -Schedule tab

8. Key in a valid interval in hours or days.

9. (Optional) Select **Send an email to the…** to send an email notification when event sources are changed after synchronization.

10. (Optional) Click **Synchronize now** to synchronize event sources immediately.

11. Click **Apply** and **OK**.

> **Note**
>
> Adding event sources manually to a synchronized group is not allowed in GFI EventsManager.

4.3 Creating a new event source group

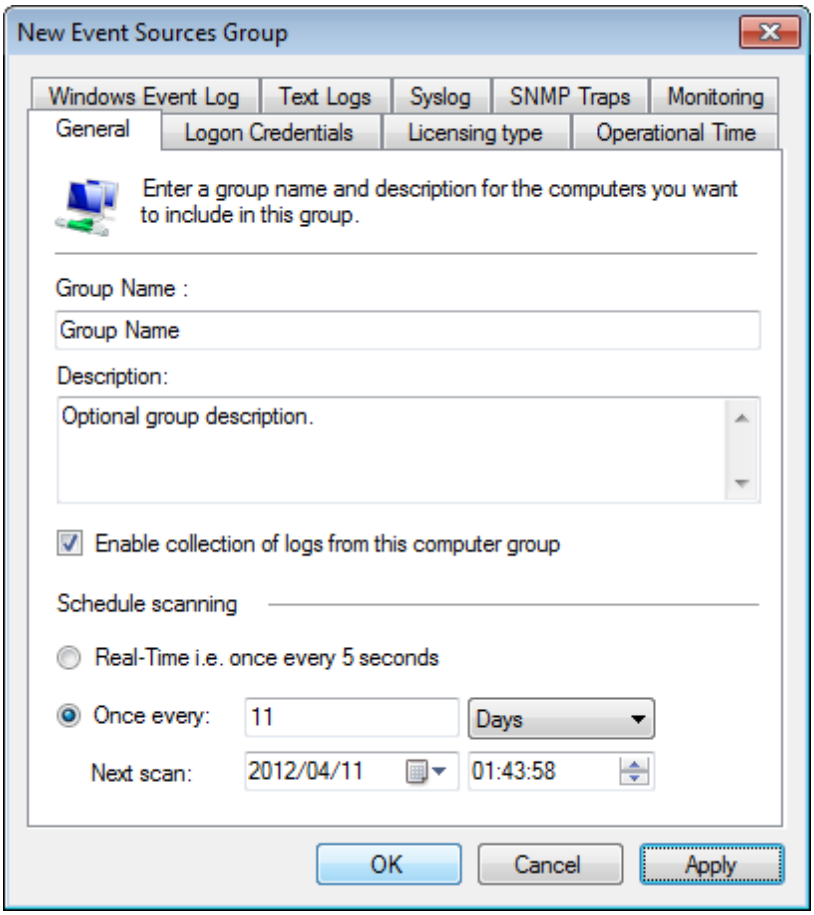
Grouping event sources into Event Source Groups improves the speed at which you configure event sources. Once an event source group is configured, every member of that particular group inherits the same settings.

To create a new event source group:

1. Click **Configuration** tab > **Event Sources** and from **Group Type**, select **Event Sources Groups**.

2. Right-click **All event sources** and select **Create group…**

3. Select the license type. Choose between **Complete** or **Active Monitoring** license. For more information refer to Configuring event source license type.



Screenshot 44: Add new event source group

4. Key in a unique name and an optional description. Select the tabs described below, and configure the available options:

Table 17: Event source group options

Tab Name	Description
General	Enable collection of events and schedule the scanning process. For more information refer to Configuring general event source properties.
Logon credentials	Configure the username and password used to login target machines and collect information. For more information refer to Configuring event source logon credentials.
Licensing type	Select the type of license to use. Select between **Active Monitoring** or **Complete**. For more information refer to Configuring event source license type.
Operational time	Configure the operational time that computers are normally used. For more information refer to Configuring event source operational time.
Monitoring	Enable GFI EventsManager active monitoring on target computers and configure the audits to perform. Monitoring checks enable administrators to identify system problems at the very early stages to prevent system down-time. For more information refer to Configuring event source monitoring.
Windows Event Log	Specify the logs to collect and configure archive settings for Windows® event logs. For more information refer to Collecting Windows® events.
Text Logs	Specify the logs to collect and configure settings for W3C/HTTP/CSV logs. This tab is only available when creating a server group. For more information refer to Collecting Text logs.
Syslog	Specify the logs to collect and configure archive settings for Syslogs. This tab is only available when creating a server group. For more information refer to Collecting Syslogs.
SNMP Traps	Specify the logs to collect and configure archive settings for SNMP Traps. This tab is only available when creating a server group. For more information refer to Collecting SNMP Traps Messages.

5. Click **Apply** and **OK**.

4.4 Configuring event source properties

GFI EventsManager allows you to customize the event source parameters to suit the operational requirements of your infrastructure. You can configure these parameters on single event sources or at event source group. Any member of a configured group inherits the same configuration, automatically.

This section contains information about:

- Configuring general event source properties
- Configuring event source logon credentials
- Configuring event source license type
- Configuring event source operational time
- Configuring event source monitoring
- Configuring event processing parameters

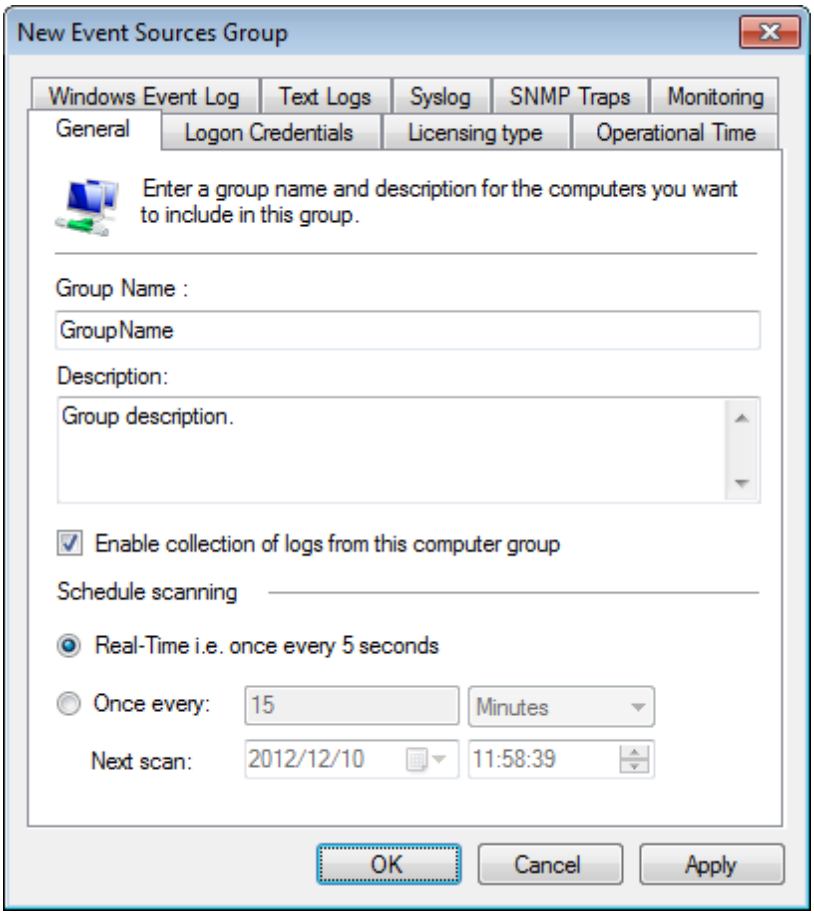
4.4.1 Configuring general event source properties

Use the **General** tab in the properties dialog to:

- Change the name of a computer group
- Enable/disable log collection and processing for the computers in a group
- Configure log collection and processing frequency.

To configure event source properties:

1. From **Configuration** tab **> Event Sources > Group Type**, select **Event Sources Groups**.
2. To configure settings of a:
   - **Computer group** - right-click on the computer group to configure, and select **Properties**
   - **Single event source** - right-click on the source to configure, and select **Properties**.



Screenshot 45: Event sources properties dialog

3. From the **General** tab, configuring the options described below:

Table 18: Event source properties - General options

Option	Description
Group Name	Key in a unique name for the computer group.
Description	(Optional) Key in a description.
Enable collection of logs from this computer group	Select/unselect this option to enable/disable event log collection from the group.
Real-Time i.e. once every 5 seconds	Select this option to check for new event logs every 5 seconds. **Note** This is not recommended if members of this group generate high volumes of event logs because it may disrupt your network performance.
Once every	Specify a custom schedule for when GFI EventsManager checks for new event logs.

4. Click **Apply** and **OK**.

4.4.2 Configuring event source logon credentials

Use the **Logon Credentials** tab in the properties dialog to:

- View logon credentials settings
- Edit logon credentials settings.

During event processing, GFI EventsManager must remotely log-on to the target computers. This is required in order to collect log data that is currently stored on the target computers and to pass this data on to the event processing engine(s).

To collect and process logs,GFI EventsManager must have administrative privileges over the target computers. By default, GFI EventsManager will log-on to target computers using the credentials of the account under which it is currently running; however, certain network environments are configured to use different credentials to log on to workstations and servers with administrative privileges.

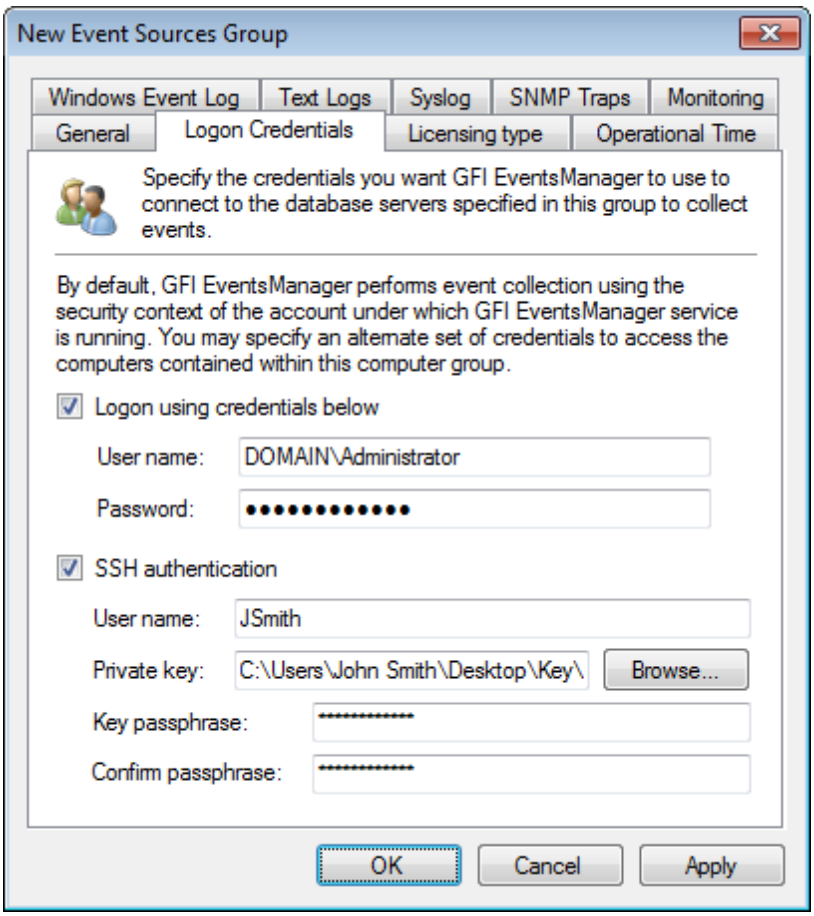
As an example, for security purposes, you might want to create an administrator account that has administrative privileges over workstations only and a different account that has administrative privileges over servers only.

To configure event source properties:

1. From **Configuration** tab **> Event Sources > Group Type**, select **Event Sources Groups**.

2. To configure settings of a:

- **Computer group** - right-click on the computer group to configure, and select **Properties**
- **Single event source** - right-click on the source to configure, and select **Properties**.



Screenshot 46: Configuring alternative logon credentials

3. Click **Logon Credentials** tab.

4. Select/unselect **Logon using credentials below** to use/stop using alternate logon credentials. Key in a username and password.

> **Note**
>
> Alternate logon credentials enable you to use different usernames and passwords to log into remote computers. You can set alternate credentials for a group of event sources or for each event source.
>
> Members of an event source group can be configured to inherit credentials from the parent group.

5. Select/unselect **SSH authentication** to use/stop using SSH authentication.

> **Note**
>
> SSH uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user, if necessary. This is a security protocol for Linux and Unix based computers.

6. Click **Browse...** to select the **Private key** file.
7. Key in the **key passphrase** and reenter it for confirmation.
8. Click **Apply** and **OK**.

4.4.3 Configuring event source license type

The **Licensing type** tab is used to configure the licensing mode of an event source or event group. This determines the type of logs that must be collected from the configured source/group. The following table describes the available license types:

Table 19: License types

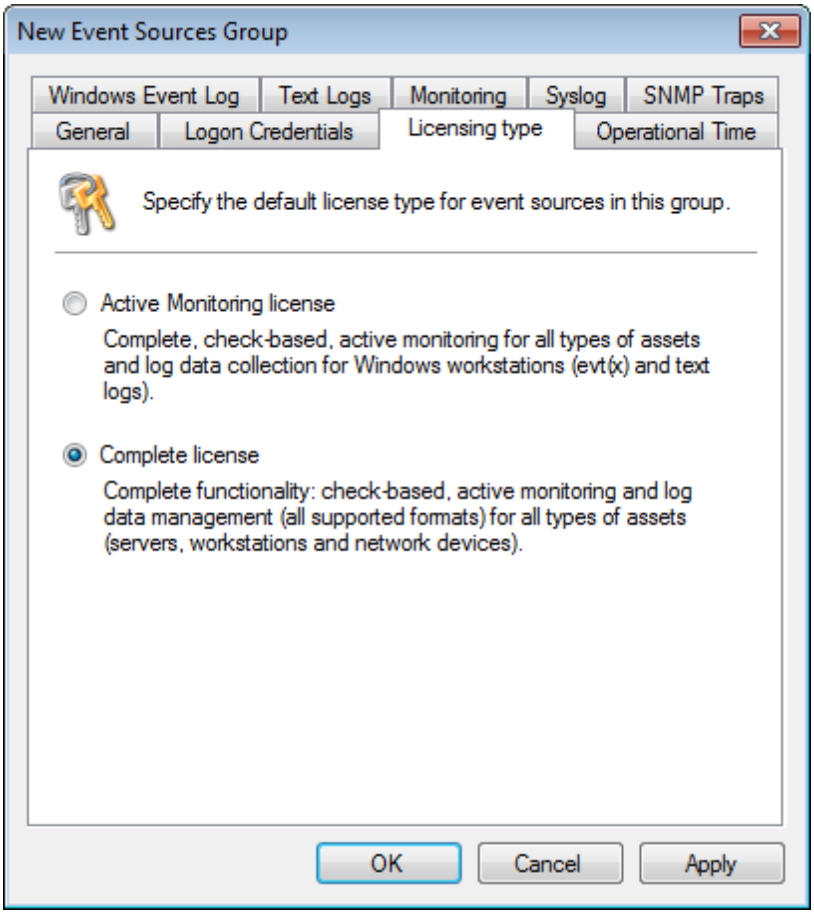
License Type	Description
Active Monitoring license	This license enables you to collect and process: » Microsoft® Windows® Event Logs » Text logs, such as W3C, CSV, XML, DHCP, SAP Logs, SKIDATA Logs and Custom logs from Windows® and non-Windows® workstations » Active Monitoring event logs If Windows® Server is detected on a source using this license, event log processing is disabled.
Complete license	Enables full functionality and support for Windows® and non-Windows® based servers, workstations and network devices. Use this license to collect and process: » Microsoft® Windows® Event Logs » Text logs, such as W3C, CSV, XML, DHCP, SAP Logs, SKIDATA Logs and Custom logs from Windows® and non-Windows® workstations » Active Monitoring event logs » SNMP Traps Messages » Syslogs » Custom Logs » SQL Server® Audits » Oracle Server Audits.

To configure event source properties:

1. From **Configuration** tab > **Event Sources** > **Group Type**, select **Event Sources Groups**.

2. To configure settings of a:

- **Computer group** - right-click on the computer group to configure, and select **Properties**
- **Single event source** - right-click on the source to configure, and select **Properties**.


New Event Sources Group
Windows Event Log
Text Logs
Monitoring
Syslog
SNMP Traps
General
Logon Credentials
Licensing type
Operational Time
Specify the default license type for event sources in this group.
Active Monitoring license
Complete, check-based, active monitoring for all types of assets and log data collection for Windows workstations (evt(x) and text logs).
Complete license
Complete functionality: check-based, active monitoring and log data management (all supported formats) for all types of assets (servers, workstations and network devices).
OK
Cancel
Apply

Screenshot 47: Configuring event source license type

3. Click **Licensing type** tab and select the license you want to use for the event source or group that is being configured.

4. Click **Apply** and **OK**.

4.4.4 Configuring event source operational time

GFI EventsManager includes an Operational Time option through which you specify the normal working hours of your event source groups. This is required so that GFI EventsManager can keep track of the events that occur both during and outside working hours.

Use the operational time information for forensic analysis; to identify unauthorized user access, illicit transactions carried outside normal working hours and other potential security breaches that might be taking place on your network.

Operational time is configurable on computer group basis. This is achieved by marking the normal working hours on a graphical operational time scale which is divided into one hour segments.

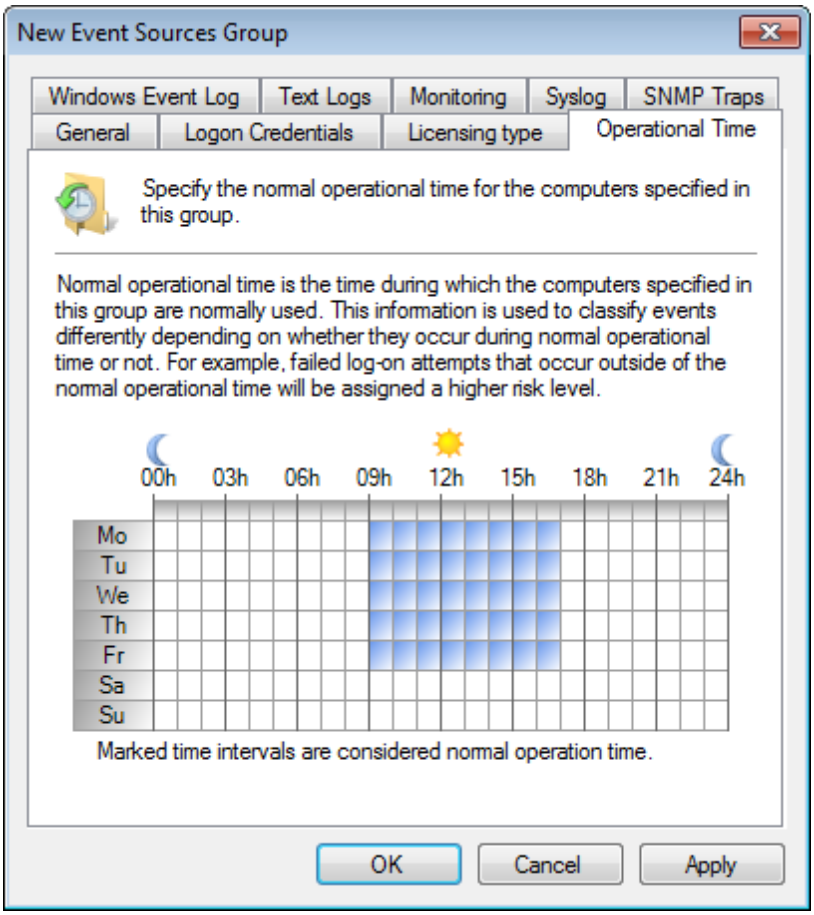
To configure event source properties:

1. From **Configuration** tab > **Event Sources** > **Group Type**, select **Event Sources Groups**.

2. To configure settings of a:

» **Computer group** - right-click on the computer group to configure, and select **Properties**

» **Single event source** - right-click on the source to configure, and select **Properties**.



Screenshot 48: Specify operational time

3. From **Operational Time** tab, mark the time intervals of your normal working hours.

> **Note**
>
> Cells marked blue represent your normal working hours.

4. Click **Apply** and **OK**.

4.4.5 Configuring event source monitoring

GFI EventsManager is able to collect additional information about your event sources through Active Monitoring. These checks generate specific events which in turn, trigger real-time notifications or execute an action.

For example, when monitoring **CPU usage** checks, GFI EventsManager queries that event source and detects whether the target machine is performing at the specified CPU usage levels.

> **Note**
>
> For more information refer to Active Monitoring.

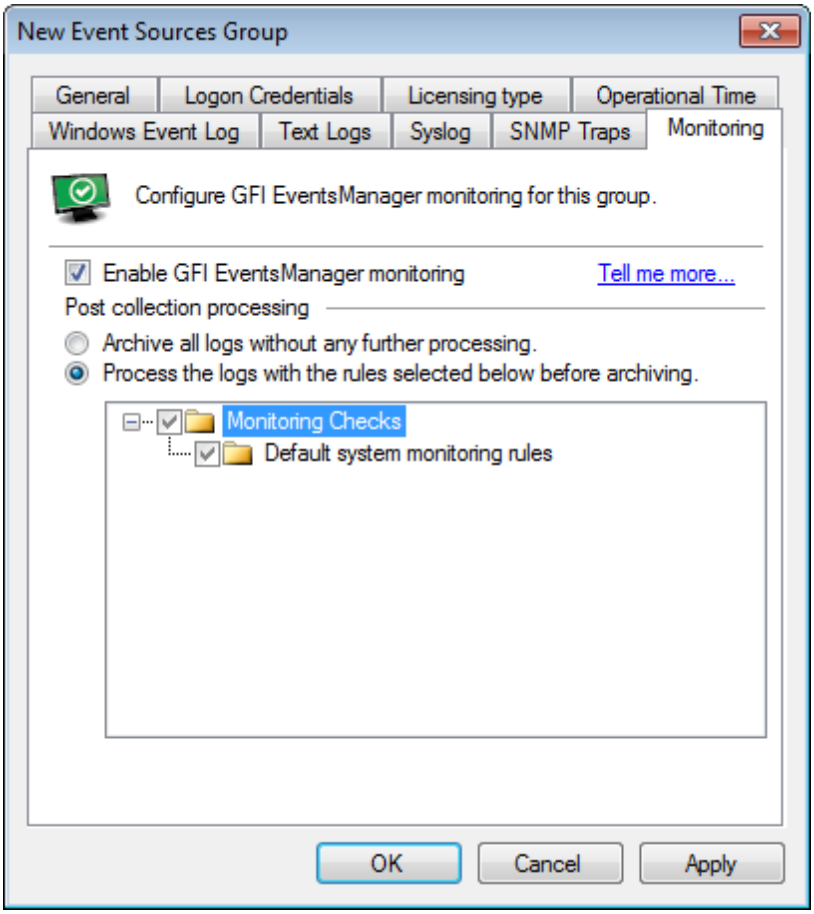
To configure event source properties:

1. From **Configuration** tab > **Event Sources** > **Group Type**, select **Event Sources Groups**.

2. To configure settings of a:

» **Computer group** - right-click on the computer group to configure, and select **Properties**

» **Single event source** - right-click on the source to configure, and select **Properties**.



Screenshot 49: Event source properties - Monitoring tab

3. From **Monitoring** tab, configure the options described below:

Table 20: Event source monitoring options

Option	Description
Inherit event log collection and processing from parent group	This option is available when enabling monitoring on a single event source. If you enabled monitoring on the group containing the event source, leave this option selected to obtain the same settings.
Enable GFI EventsManager monitoring	Select/unselect this option to enable/disable Active Monitoring processing.
Perform the following checks	Expand the list of checks and select the ones which you want to apply to your event source/event source group. For information about creating monitoring checks, refer to Creating a new monitoring check.

Option	Description
Archive all logs without any further processing	Select this option to store events without applying any further checks (from Events Processing Rules).
Process the logs with the rules selected below before archiving	Expand the list of rules which are applied to the collected logs. GFI EventsManager enables you to create custom rules and configure them to trigger when one of the active monitoring check generates an event. Then, through the configuration of the selected Event Processing Rule, actions are executed and/or alerts are generated. Once a monitoring check is enabled, browse for the event that it generates and create a rule based on that event. For more information refer to Creating new rules from existing events.

4. Click **Apply** and **OK**.

4.4.6 Configuring event processing parameters

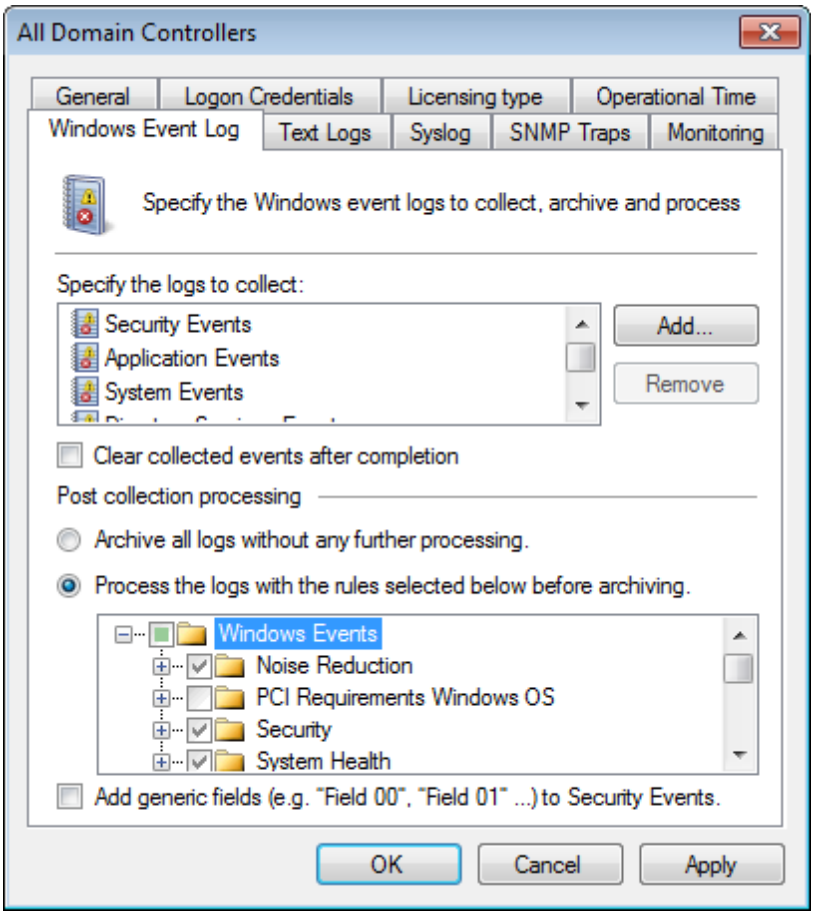
Event processing parameters are enabled only for event sources/groups licensed as Servers. Server event sources posses more settings than normal workstations, in order to collect Windows® event logs, Text logs, Syslogs and SNMP Traps.

To configure event source properties:

1. From **Configuration** tab **>** **Event Sources** **>** **Group Type**, select **Event Sources Groups**.

2. To configure settings of a:

- **Computer group** - right-click on the computer group to configure, and select **Properties**
- **Single event source** - right-click on the source to configure, and select **Properties**.



Screenshot 50: Event processing configuration tabs

3. Use the **Windows Event Log**, **Text Logs**, **Syslog** and **SNMP Traps** tabs configure the required event processing parameters.

4. Click **Apply** and **OK**.

> **Note**
>
> For more information, refer to:
>
> - Collecting Windows® Event Logs
> - Collecting Text logs
> - Collecting Syslogs
> - Collecting SNMP Traps.

4.5 Database sources

GFI EventsManager can monitor and process events from database servers. Database event sources require specific configuration settings to collect and process events generated by database activity. GFI EventsManager is able to audit and monitor activity from the following database servers:

- Microsoft® SQL Server®
- Oracle Server

4.5.1 Microsoft® SQL Server® Sources

This section contains information about:

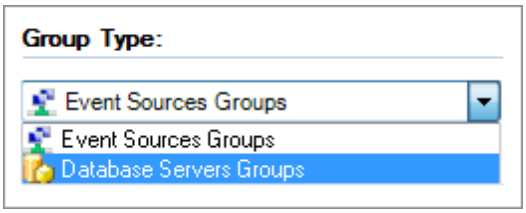
- Creating a new Microsoft® SQL Server® group
- Adding a new Microsoft® SQL Server® event source

Creating a new Microsoft® SQL Server® group

To create a Microsoft® SQL Server® group:

1. Click **Configuration** tab > **Event Sources**.

2. From **Group Type**, select **Database Servers Groups**.



Screenshot 51: Database Servers Groups

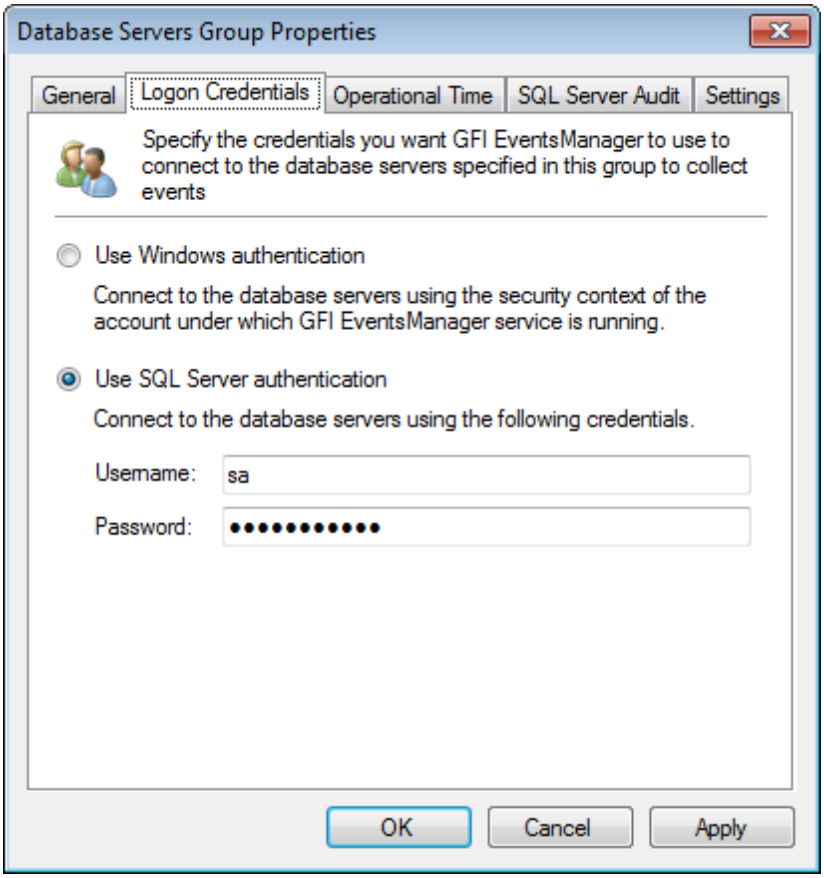
3. From **Groups**, right-click **Microsoft® SQL Server®** and select **Create group...**

4. Select **Microsoft® SQL Server®** as the server type and from **General** tab configure the options described in below:

Table 21: Microsoft® SQL Database group: General tab

Option	Description
Group Name	Key in a group name to identify the Microsoft® SQL Server® group.

Option	Description
Description	(Optional) Key in a description.
Collects logs from the database servers included in this group	Enable option to collect database events from all servers in this group.

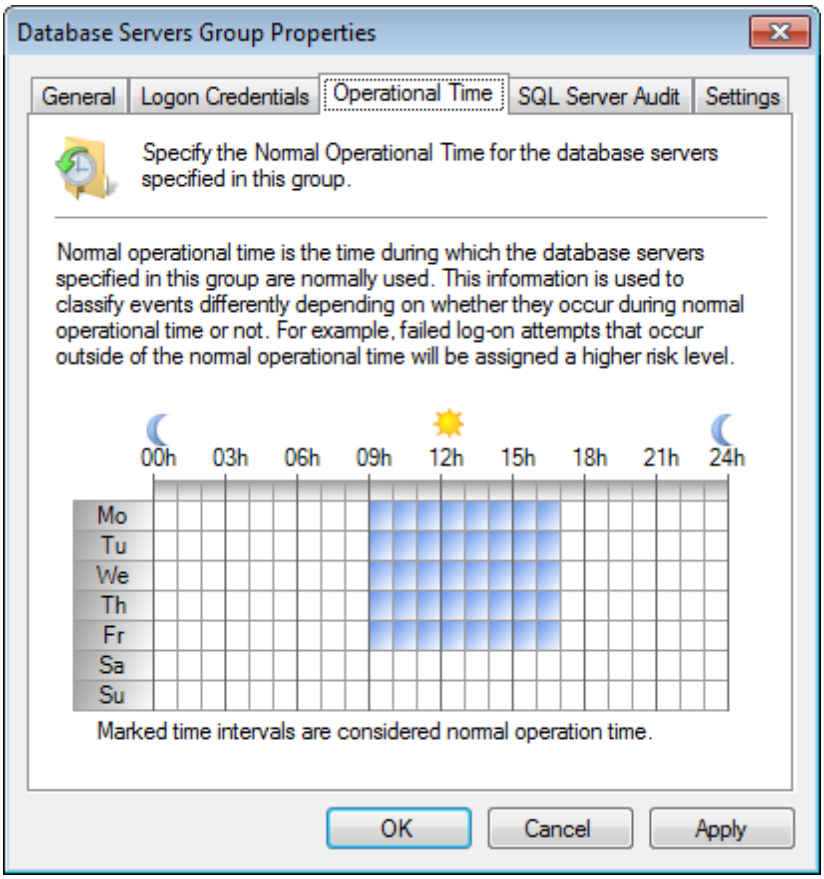

Database Servers Group Properties
General
Logon Credentials
Operational Time
SQL Server Audit
Settings
Specify the credentials you want GFI EventsManager to use to connect to the database servers specified in this group to collect events
Use Windows authentication
Connect to the database servers using the security context of the account under which GFI EventsManager service is running.
Use SQL Server authentication
Connect to the database servers using the following credentials.
Username:
sa
Password:
OK
Cancel
Apply

Screenshot 52: Configure logon settings from the Logon Credentials tab

4. Select **Logon Credentials** tab and configure the options described below:

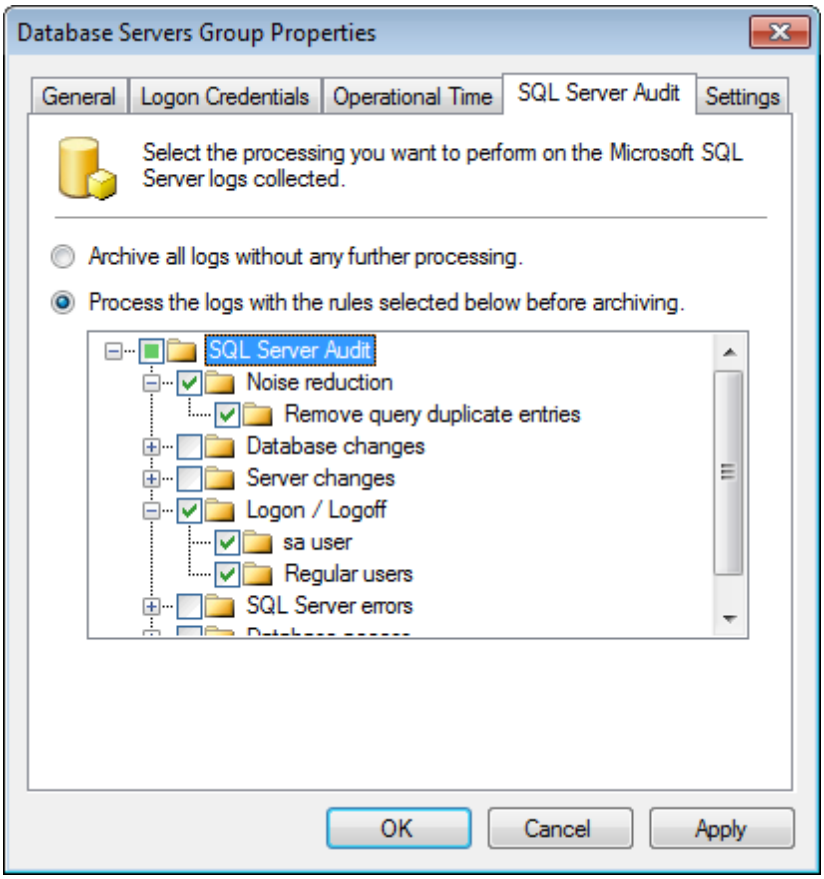
Table 22: Microsoft® SQL Database group: Logon Credentials

Option	Description
Use Windows authentication	Connect to the Microsoft® SQL Database using windows authentication.
Use SQL Server® authentication	Connect to Microsoft® SQL Database using a Microsoft® SQL Database user account. Key in a username and password.



Screenshot 53: Configure the normal working hours from Operational Time tab

5. Select **Operational Time** and configure the operational time when the database is normally used. Marked time intervals are considered normal working hours.

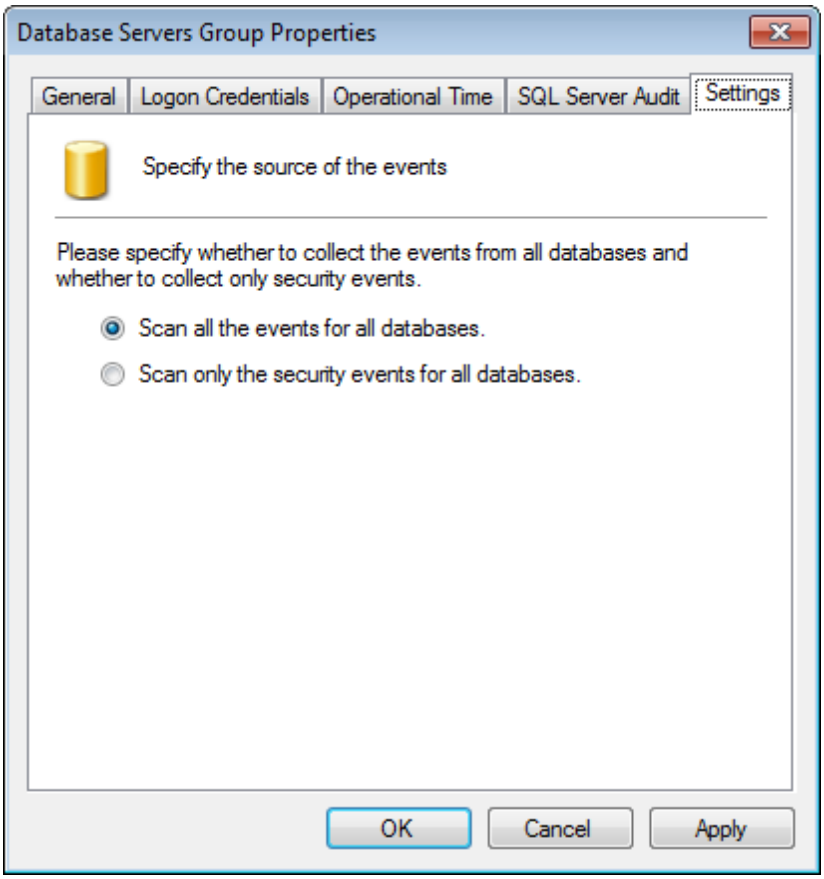


Screenshot 54: Configure SQL Server Auditing from SQL Server Audit tab

6. Select **SQL Server® Audit** tab and configure the options described below:

Table 23: Microsoft® SQL Database group -SQL Server® Audit

Option	Description
Archive all logs without further processing	Archive events in GFI EventsManager database backend without applying processing rules.
Process the logs with the rules selected below before archiving	Specify the rules to perform before archiving events in GFI Events-Manager database backend.


Database Servers Group Properties
General
Logon Credentials
Operational Time
SQL Server Audit
Settings
Specify the source of the events
Please specify whether to collect the events from all databases and whether to collect only security events.
Scan all the events for all databases.
Scan only the security events for all databases.
OK
Cancel
Apply

7. Select **Settings** tab and configure the options described in below:

Table 24: Microsoft® SQL Database group - Settings

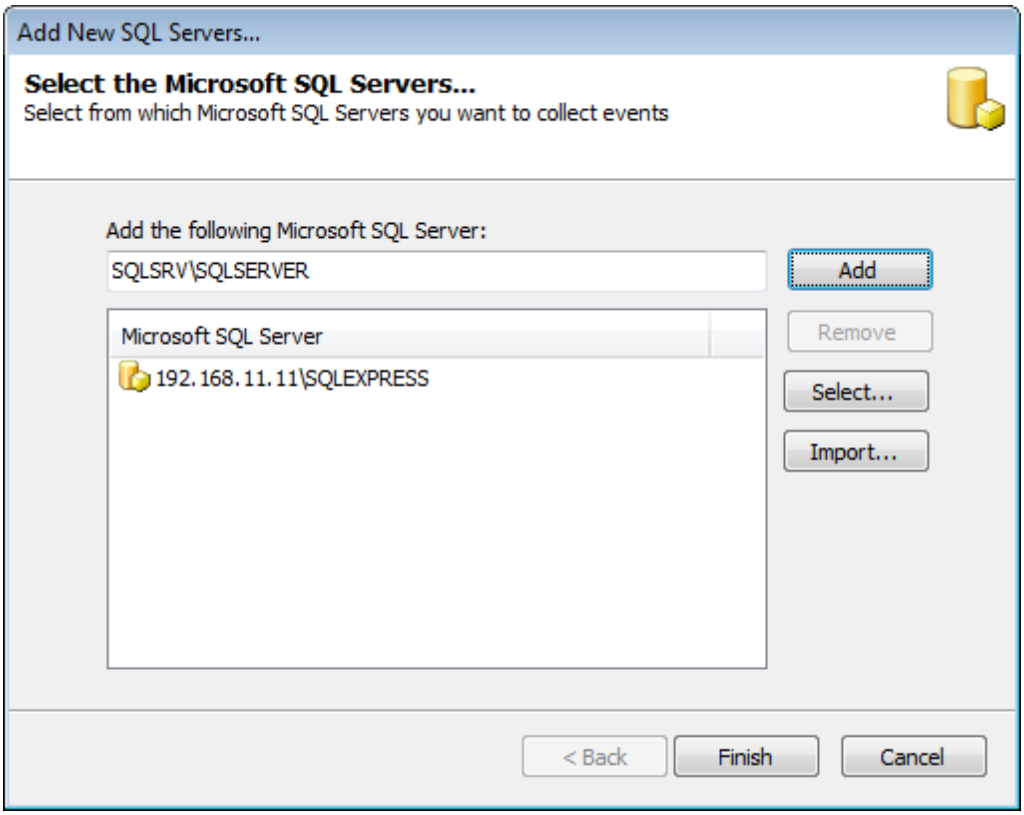
Option	Description
Scan all the events for all databases	All Microsoft® SQL Server® events are collected and processed by GFI EventsManager.
Scan only security events for all databases	Only security events are collected and processed by GFI EventsManager.

8. Click **Apply** and **OK**.

Adding a new Microsoft® SQL Server® event source

To add a new Microsoft® SQL Server® source:

1. Right-click a database group and select **Add new SQL Server®...**



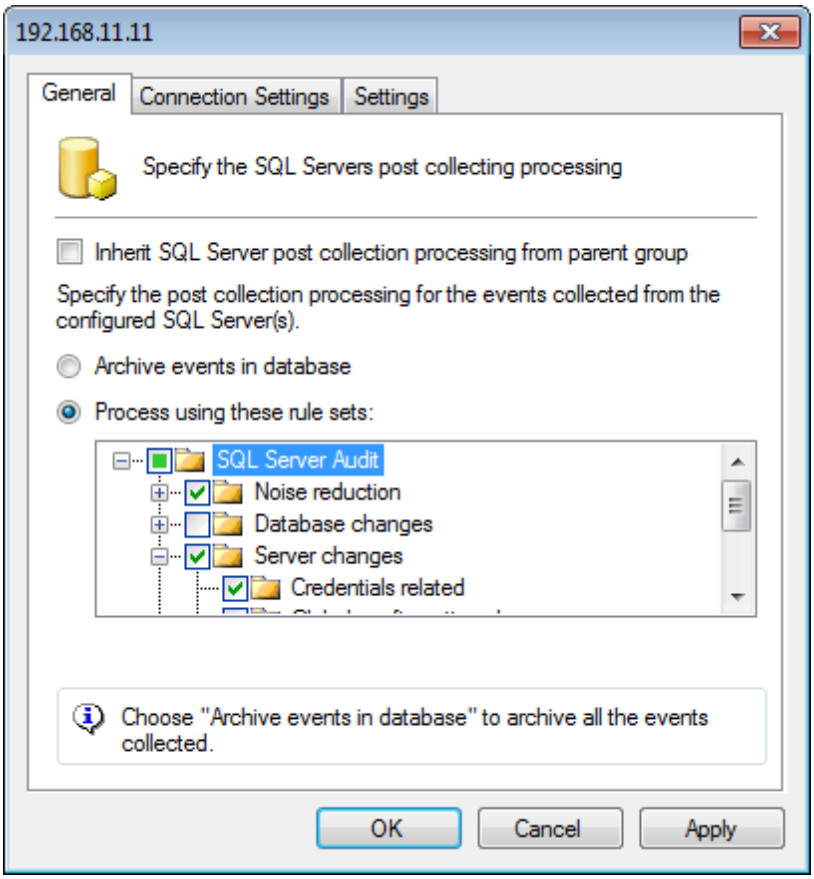
Screenshot 55: Add new Microsoft® SQL server

2. Key in the server name or IP and click **Add**.

> **Note**
>
> Use **Select** and **Import** to search the network for SQL Server® or import list of SQL servers from a text file respectively.

3. Click **Finish** and the Add New SQL Servers dialog closes.

4. From **Groups**, select **SQL Servers** and from the right pane, double-click the new Microsoft® SQL Database instance.

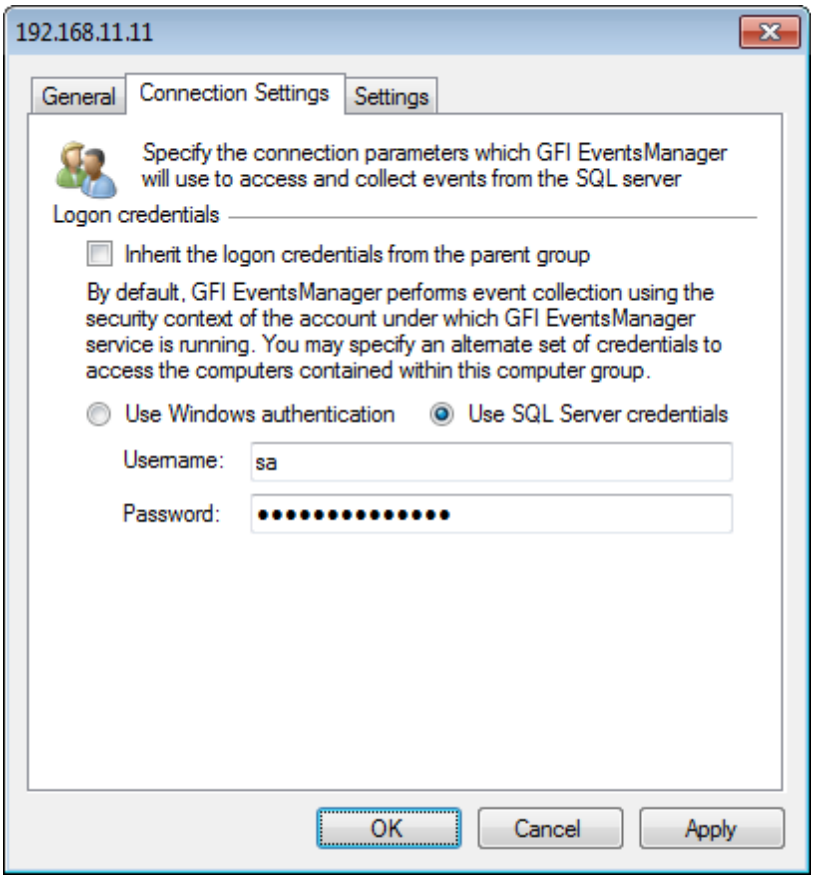


Screenshot 56: Microsoft® SQL Database properties: General tab

5. From **General** tab, configure the options described below:

Table 25: Microsoft® SQL Database - General tab options

Option	Description
Inherit SQL Server post collecting processing from parent group	Inherits all settings from the parent group.
Archive events in database	Archive events in GFI EventsManager database backend without applying processing rules.
Process using these rule sets	Specify the rules to perform before archiving events in GFI Events-Manager database backend.

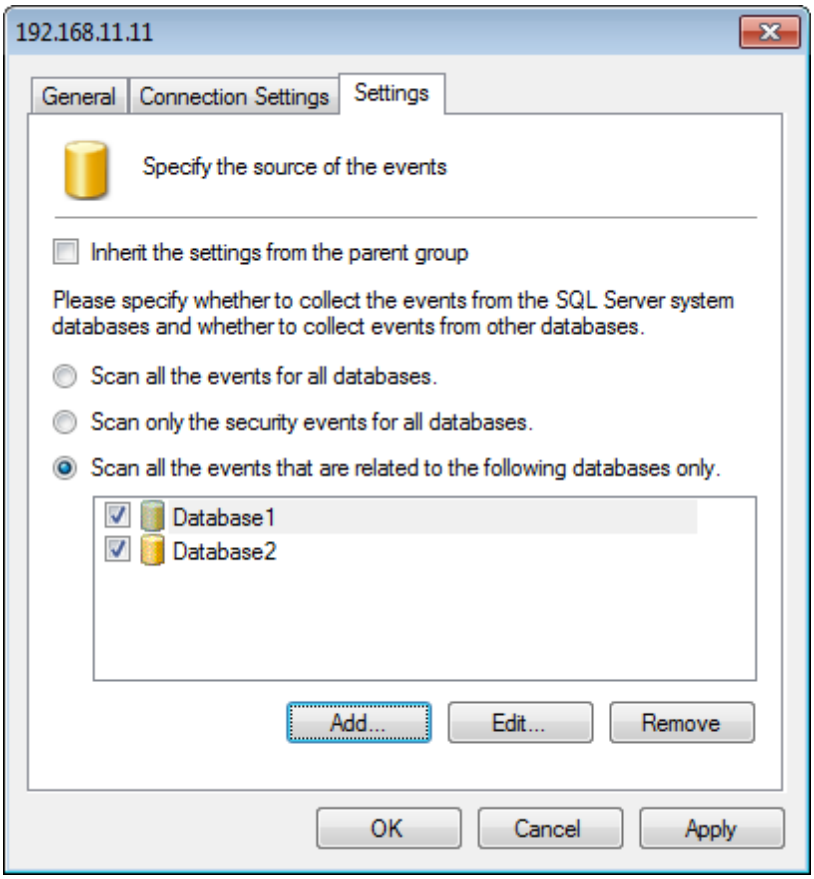

192.168.11.11
General
Connection Settings
Settings
Specify the connection parameters which GFI EventsManager will use to access and collect events from the SQL server
Logon credentials
Inherit the logon credentials from the parent group
By default, GFI EventsManager performs event collection using the security context of the account under which GFI EventsManager service is running. You may specify an alternate set of credentials to access the computers contained within this computer group.
Use Windows authentication
Use SQL Server credentials
Username:
sa
Password:
OK
Cancel
Apply

Screenshot 57: Microsoft® SQL Database properties: Connection Settings tab

6. Select **Connection Settings** and configure the options described below:

Table 26: Microsoft® SQL Database - Connection Settings tab

Option	Description
Inherit the logon credentials from the parent group	Select this option to inherit login settings from the parent group.
Use Windows authentication	Connect to Microsoft® SQL Database using windows authentication.
Use SQL Server credentials	Connect to Microsoft® SQL Database using a Microsoft® SQL Database user account. Key in a username and password.


192.168.11.11
General
Connection Settings
Settings
Specify the source of the events
Inherit the settings from the parent group
Please specify whether to collect the events from the SQL Server system databases and whether to collect events from other databases.
Scan all the events for all databases.
Scan only the security events for all databases.
Scan all the events that are related to the following databases only.
Database1
Database2
Add...
Edit...
Remove
OK
Cancel
Apply

Screenshot 58: Microsoft® SQL Database properties: Settings tab

7. Select **Settings** tab and configure the options described below:

Table 27: Microsoft® SQL Database - Settings tab options

Option	Description
Inherit the settings from the parent group	Inherits settings from the parent group.
Scan all the events for all databases	Scan all databases and collect all events from the Microsoft® SQL Server®.
Scan only the security events for all databases	Scan all databases and collect only security events from the Microsoft® SQL Server®.
Scan all the events that are related to the following databases only	Collect all events from the selected databases. Use Add, Edit and Remove to manage database sources.

8. Click **Apply** and **OK**.

4.5.2 Oracle server sources

GFI EventsManager enables you to collect and process events generated by Oracle Relational database management systems. The following audits are collected and processed by GFI EventsManager:

Table 28: Oracle Server supported audits

Audit	Description
Session auditing	Audit user sessions and database access.
Statement auditing	Audit processed SQL statements.
Object auditing	Audit queries and statements related to specific objects.

The following Oracle Database versions are supported:

- Oracle Database 9i
- Oracle Database 10g
- Oracle Database 11g

This section contains information about:

- Pre-configuration settings for Oracle Servers event sources
- Creating a new Oracle Server group
- Adding a new Oracle Server event source

Pre-configuration settings for Oracle Servers event sources

Before adding Oracle Server event sources, follow the steps below on each Oracle Server instance you want to monitor:

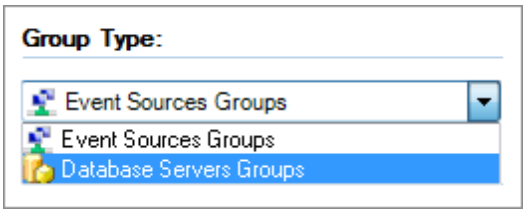
Table 29: Oracle Server configuration stages

Pre-configuration Step	Description
Step 1	Ensure the logon credentials used to connect, set audits and access the audit table has the necessary permissions.
Step 2	Enable auditing on the Oracle Server by changing startup parameters. To enable auditing: 1. Startup parameters for the Oracle servers are stored in: `<Oracle Home Directory>\admin\<Oracle SID>\pfile\init.ora.` 2. Locate and open the parameters file using a text editor. 3. Locate **AUDIT_TRAIL** parameter and change the default value to '**db**' or '**db_extended**' ('db, extended' on latest versions of Oracle). 4. Save and restart the Oracle server.

Adding a new Oracle Server group

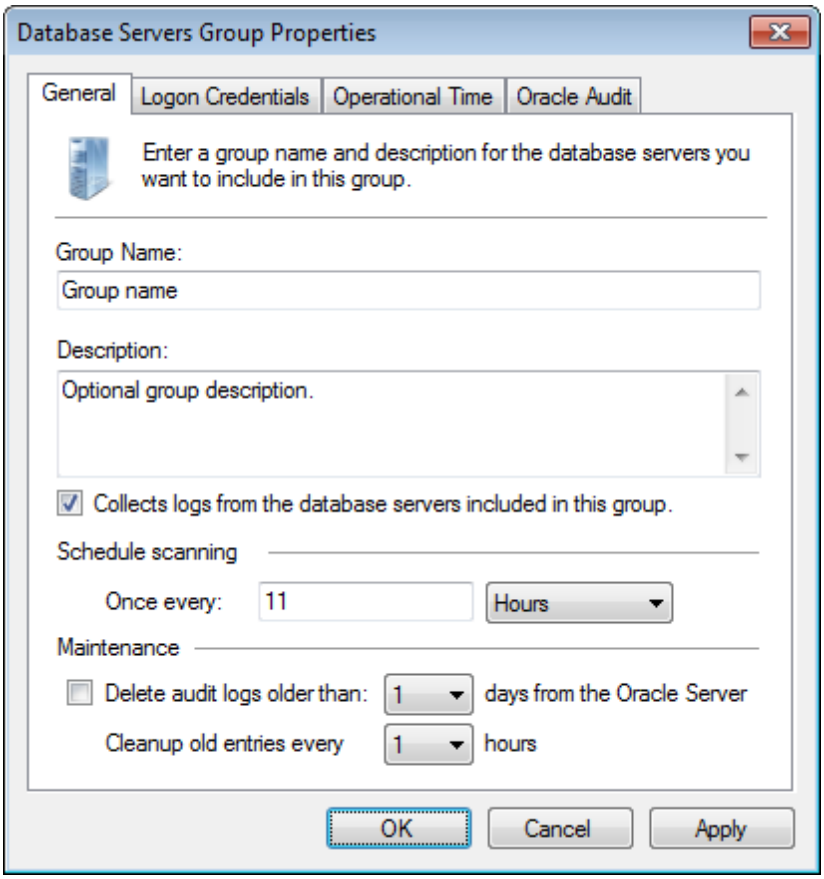
To add a new Oracle Database group:

1. Click **Configuration** tab > **Event Sources**.
2. From **Group Type**, select **Database Servers Groups**.



Screenshot 59: Database Servers Groups

3. From **Groups**, right-click **Oracle Servers** and select **Create group...**

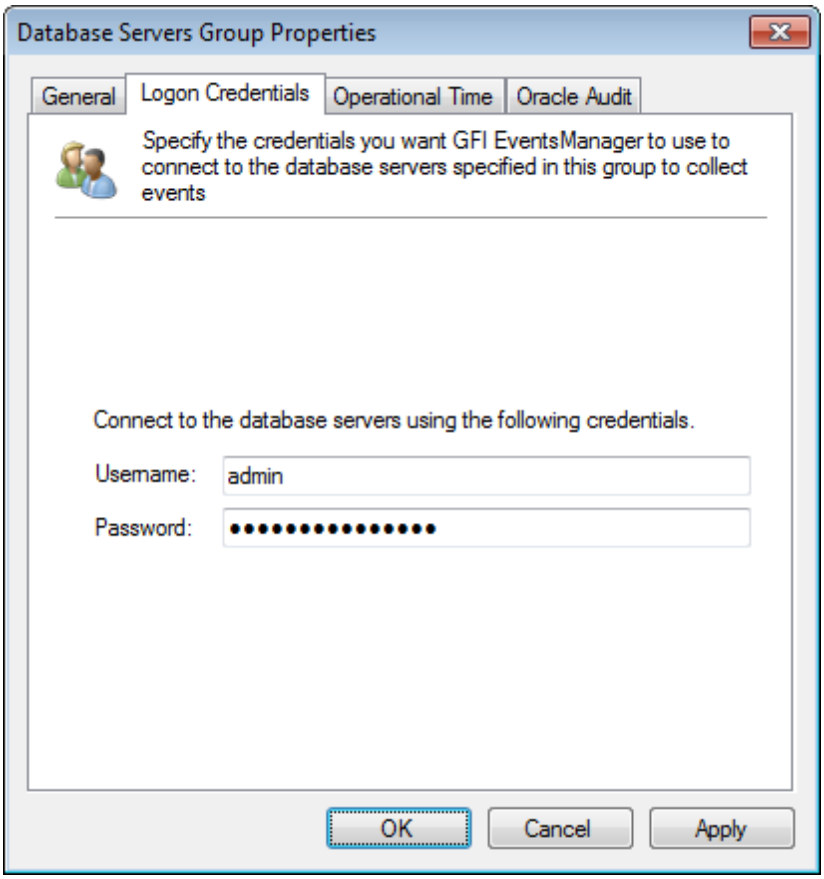


Screenshot 60: Oracle Database group - General tab

4. From **General** tab, configure the options described in below:

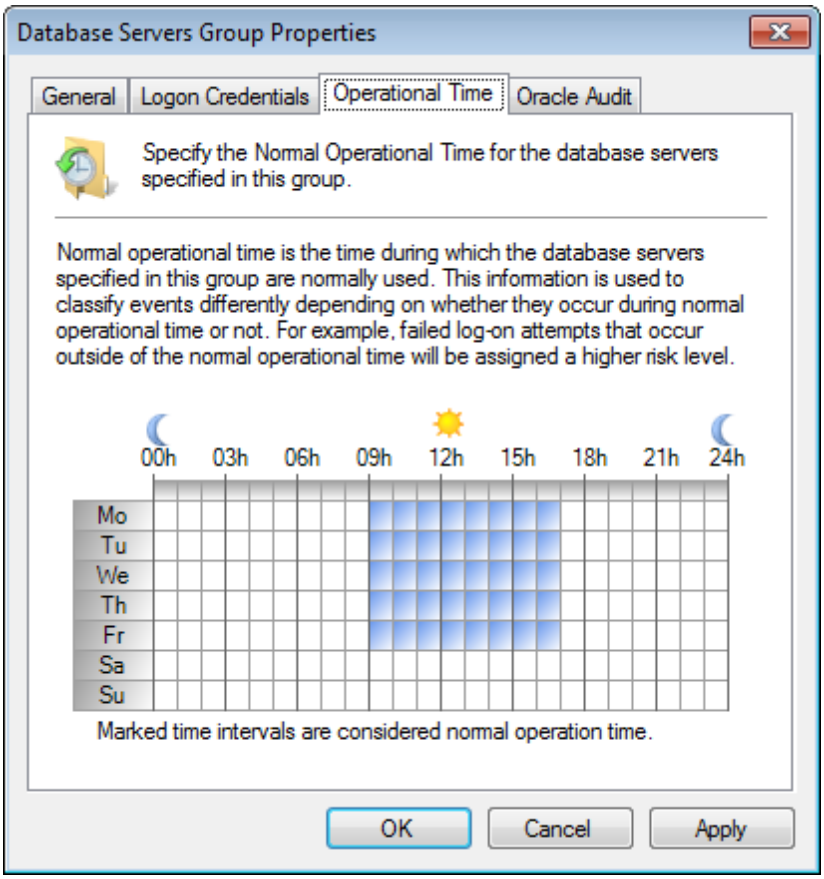
Table 30: Oracle Database group - General tab

Option	Description
Group Name	Key in a group name to identify the Oracle Database group.
Description	Optionally, key in a description.
Collects logs from the database servers included in this group	Collects events from the event sources in the Oracle group. Once this option is enabled, configure the Schedule scanning and Maintenance options.
Schedule scanning	Specify the frequency to collect events on a pre-defined schedule.
Maintenance	Oracle audit events are stored in a specific audit table on the Oracle server. To prevent excessive audit table growth, configure the options in this section to delete audit logs and old entries on a pre-defined time.



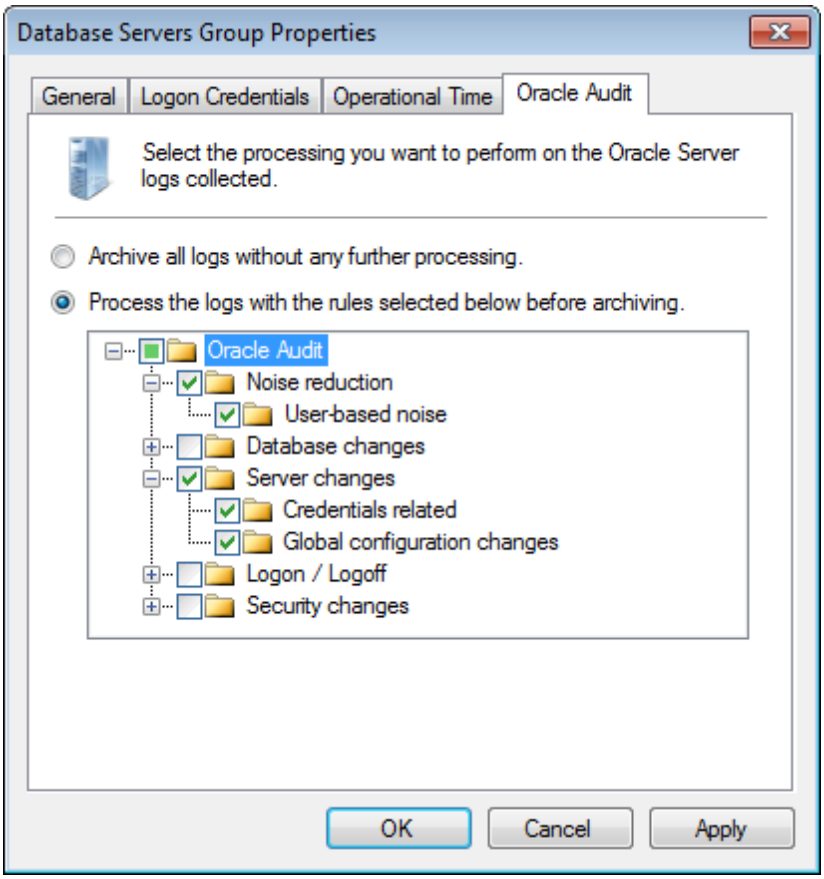
Screenshot 61: Oracle Database group - Logon Credentials tab

5. Select **Logon Credentials** tab and key in a valid username and password to connect to the Oracle server.


Database Servers Group Properties
General
Logon Credentials
Operational Time
Oracle Audit
Specify the Normal Operational Time for the database servers specified in this group.
Normal operational time is the time during which the database servers specified in this group are normally used. This information is used to classify events differently depending on whether they occur during normal operational time or not. For example, failed log-on attempts that occur outside of the normal operational time will be assigned a higher risk level.
00h
03h
06h
09h
12h
15h
18h
21h
24h
Mo
Tu
We
Th
Fr
Sa
Su
Marked time intervals are considered normal operation time.
OK
Cancel
Apply

Screenshot 62: Oracle Database group - Operational Time tab

6. Select **Operational Time** tab and configure the normal operational time of the Oracle Database servers in this group.



Screenshot 63: Oracle Database group - Oracle Audit tab

7. Select **Oracle Audit** and configure the options described below:

Table 31: Oracle Database group - Oracle Audit

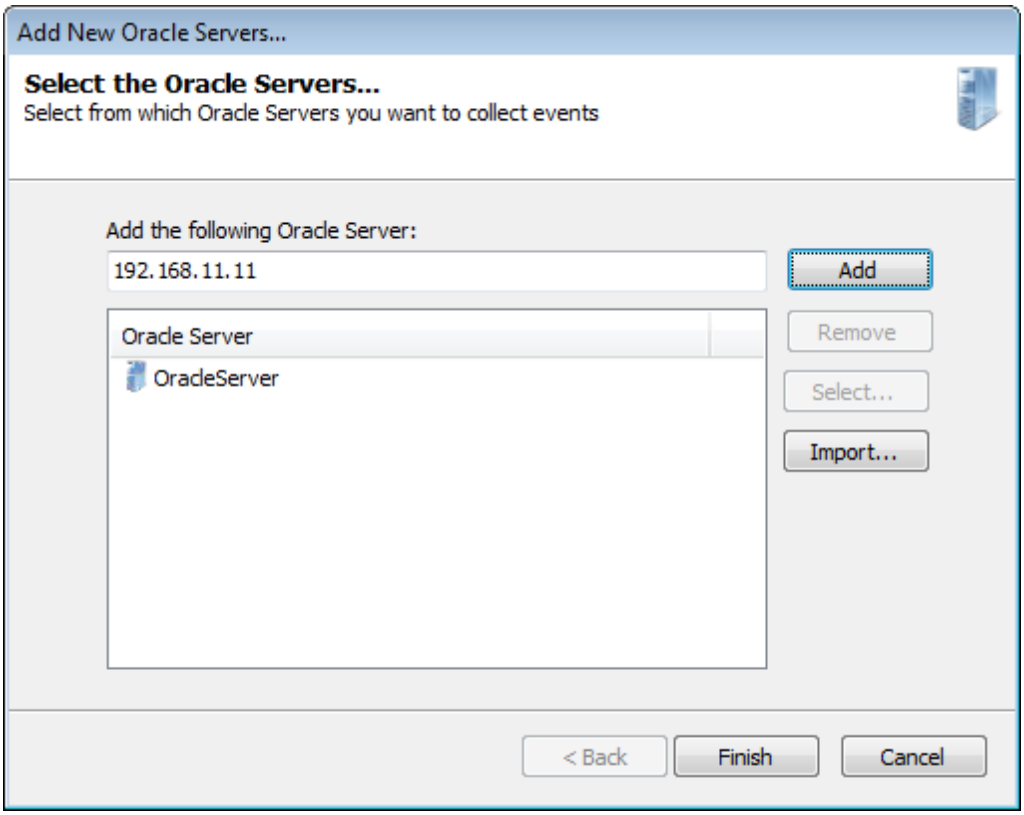
Option	Description
Archive all logs without further processing	Archive events in GFI EventsManager database backend without applying processing rules.
Process the logs with the rules selected below before archiving	Specify the rules to perform before archiving events in GFI Events-Manager database backend.

8. Click **Apply** and **OK**.

Adding a new Oracle Server event source

To add a new Oracle Database to a database group:

1. Right-click an Oracle Server group and select **Add new Oracle Server...**

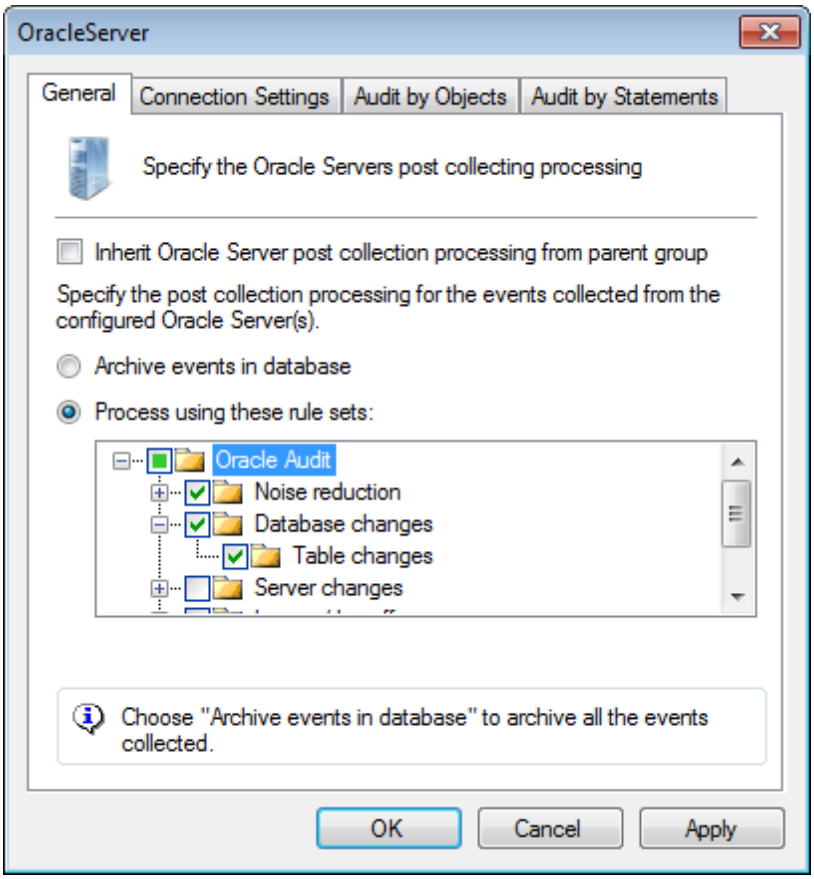


Screenshot 64: Add new Oracle server

2. Key in the server name or IP and click **Add**.

3. Click **Finish** and the Add New Oracle Servers dialog closes.

> **Note**
>
> Use **Select** and **Import** to search the network for SQL Server® or import list of SQL Server® from a text file respectively.

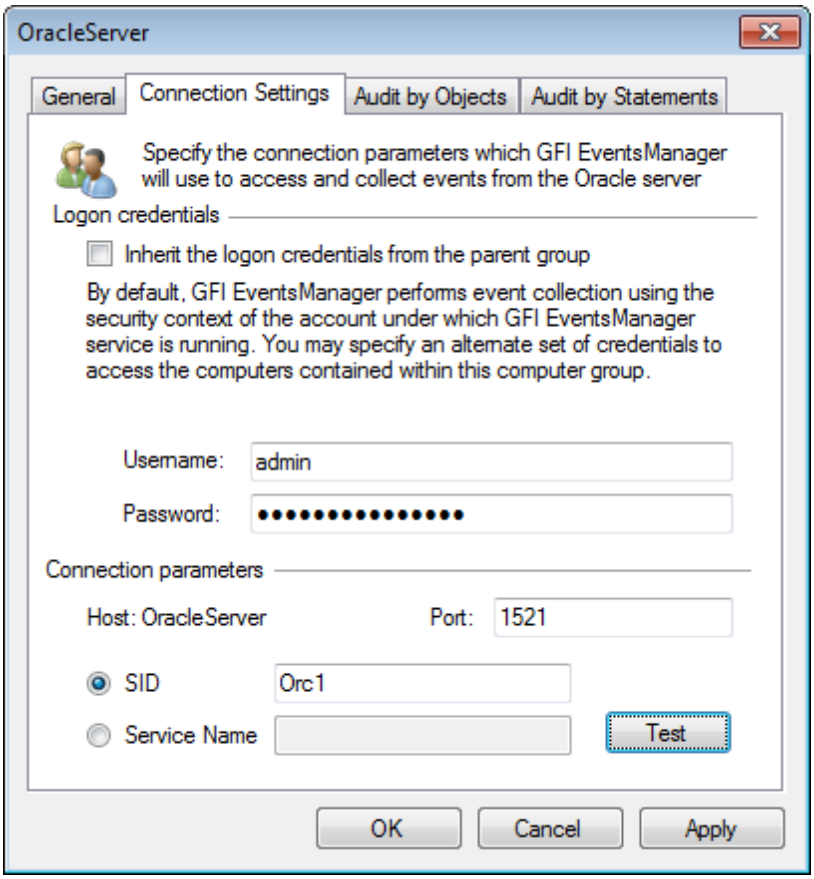


Screenshot 65: Oracle Server properties - General tab

4. From the right pane, double-click the new oracle server event source and configure the options described below:

Table 32: Oracle Server properties - General tab

Option	Description
Inherit Oracle Server post collecting processing from parent group	Select to inherit all settings from the parent group.
Archive events in database	Archive events in GFI EventsManager database backend without applying processing rules.
Process using these rule sets	Specify the rules to perform before archiving events in GFI Events-Manager database backend.

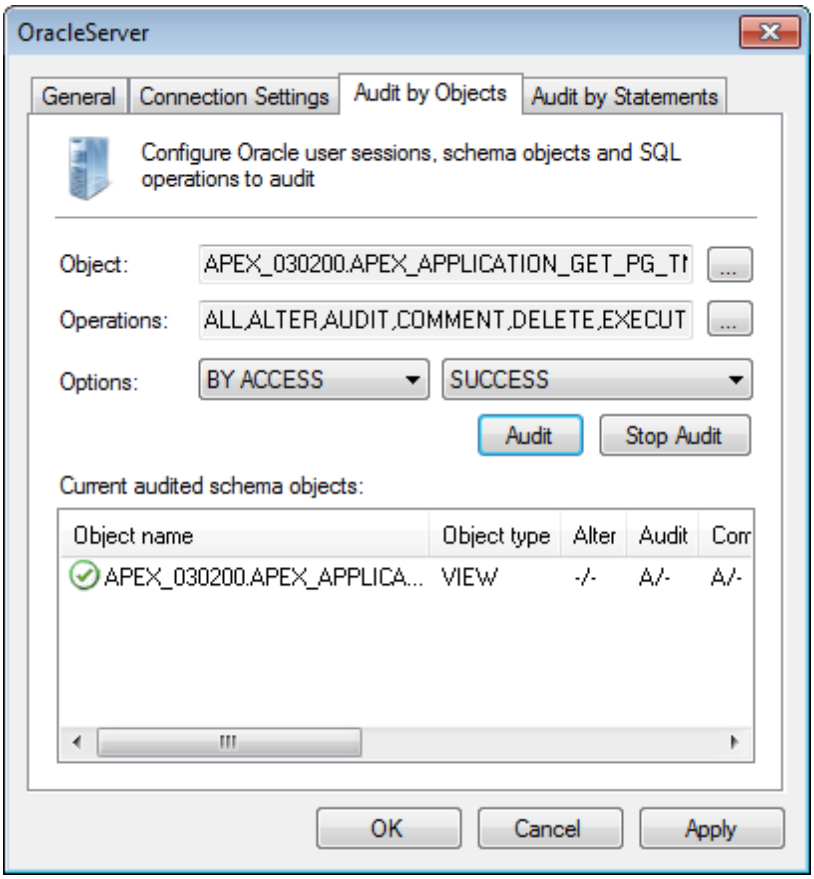

OracleServer
General
Connection Settings
Audit by Objects
Audit by Statements
Specify the connection parameters which GFI EventsManager will use to access and collect events from the Oracle server
Logon credentials
Inherit the logon credentials from the parent group
By default, GFI EventsManager performs event collection using the security context of the account under which GFI EventsManager service is running. You may specify an alternate set of credentials to access the computers contained within this computer group.
Username:
admin
Password:
Connection parameters
Host: OracleServer
Port:
1521
SID
Orc1
Service Name
Test
OK
Cancel
Apply

Screenshot 66: Oracle Server properties - Connection Settings tab

5. Select **Connection Settings** and configure the options described below:

Table 33: Oracle Server properties - Connection Settings tab

Option	Description
Inherit the logon credentials from the parent group	Select to inherit login settings from the parent group.
Port	Key in the port to use to connect to the Oracle Database.
SID	The SID is a unique name to identify an Oracle Database instance. Key in the SID of the database to audit.
Service Name	The Service name is the alias used to identify the Oracle Database. Key in the Service name of the database to audit.
Test	Test the connection with the Oracle Database server.

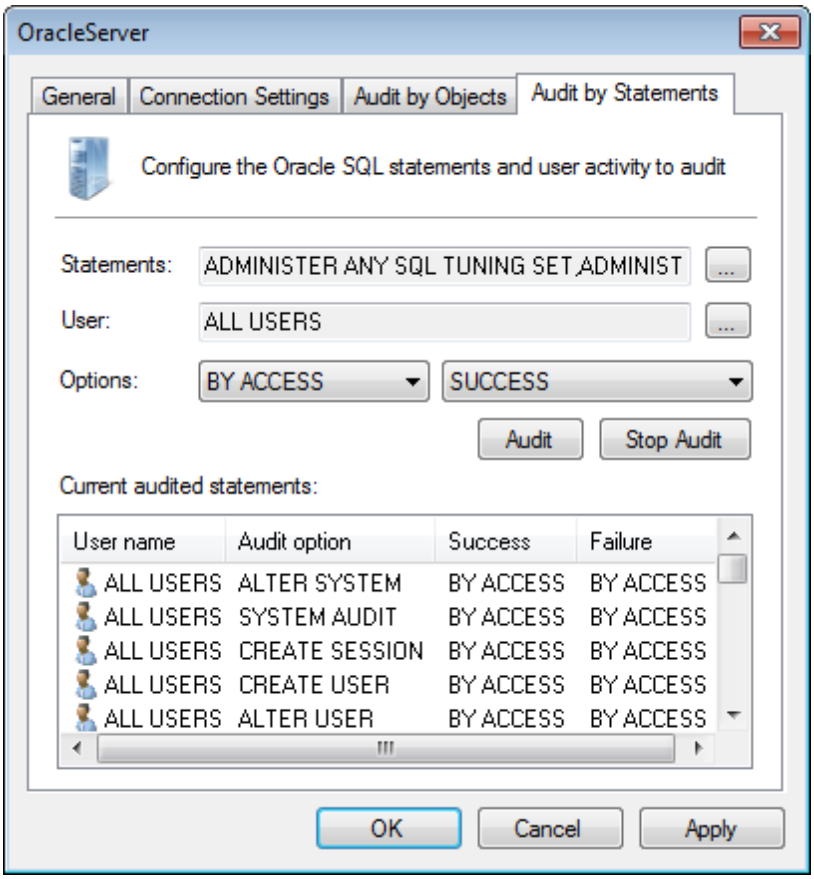


Screenshot 67: Oracle Server properties - Audit by Objects tab

6. Select **Audit by Objects** and configure the options described below:

Table 34: Oracle Server properties - Audit by Objects tab

Option	Description
Object	Click **Browse** to launch a list of available Oracle objects. Select the object to audit and click **OK**. **NOTE**: Amongst others, Oracle objects can be procedures, views, functions and tables.
Operations	Operations are actions that modify or query an object. Click **Browse** to launch a list of available operations. Select the operations to audit and click **OK**.
Options	Select the audit options: » **By Access** - Creates an audit log per object operation execution. » **By Session** - Creates an audit log per operation and per schema object. A session is the time between a connection and a disconnection to/from the database. » **Success** - Select to process only successful audits. » **Failure** - Select to process only failed audits. Oracle will create an audit log if an audit fails to complete. » **Both** - Select to process all audit logs.
Audit	Choose this option to instruct the Oracle server to start auditing the server activities corresponding to the selected parameters (like users, statements, etc.)
Stop Audit	Choose this option to instruct the Oracle server to stop auditing the server activities corresponding to the selected parameters (such as users, statements, etc.)
Current audited schema objects	A list that displays all current Oracle audited schema.



Screenshot 68: Oracle Server properties - Audit by Statements tab

7. Select **Audit by Statements** and configure the options described below:

Table 35: Oracle Server properties - Audit by Statements tab

Option	Description
Statements	Click **Browse**to launch a list of available Oracle statements. Select the Oracle statements to audit and click **OK**. **NOTE**: Amongst others, Oracle statements can be **ALTER**, **CREATE** and **SELECT** .
User	Oracle enables you to audit statements for a specific user. Click **browse** button to launch a list of available users. Select the user and click **OK**.
Options	Select audit options: » **By Access** - Creates one audit log for each statement execution. » **By Session** - Creates one audit log per user and per schema object. A session is the time between a connection and a disconnection to/from the database. » **Success** - Processes only successful audits. » **Failure** - Select option to process only failed audits. Oracle will create an audit log if an audit fails to complete. » **Both** - Select option to process all audit logs.
Audit	Choose this option to instruct the Oracle server to start auditing the server activities corresponding to the selected parameters (such as users, statements, etc.)
Stop Audit	Choose this option to instruct the Oracle server to stop auditing the server activities corresponding to the selected parameters (such as users, statements, etc.)
Current audited state-ments	A list that displays all current Oracle audited statements.

8. Click **Apply** and **OK**.

5 Collecting Event Logs

This chapter provides you with information about how to configure your event sources to apply events processing rules to collected events. Assign existing or custom events processing rules to precisely process the events wanted only.

Topics in this chapter:

5.1 Collecting Windows® event logs 100

5.2 Collecting Text logs 103

5.3 Collecting Syslogs 106

5.4 Collecting SNMP Traps Messages 110

5.5 Collecting custom logs 114

5.6 Collecting GFI LanGuard event logs 116

5.7 Collecting GFI EndPointSecurity events 121

5.1 Collecting Windows® event logs

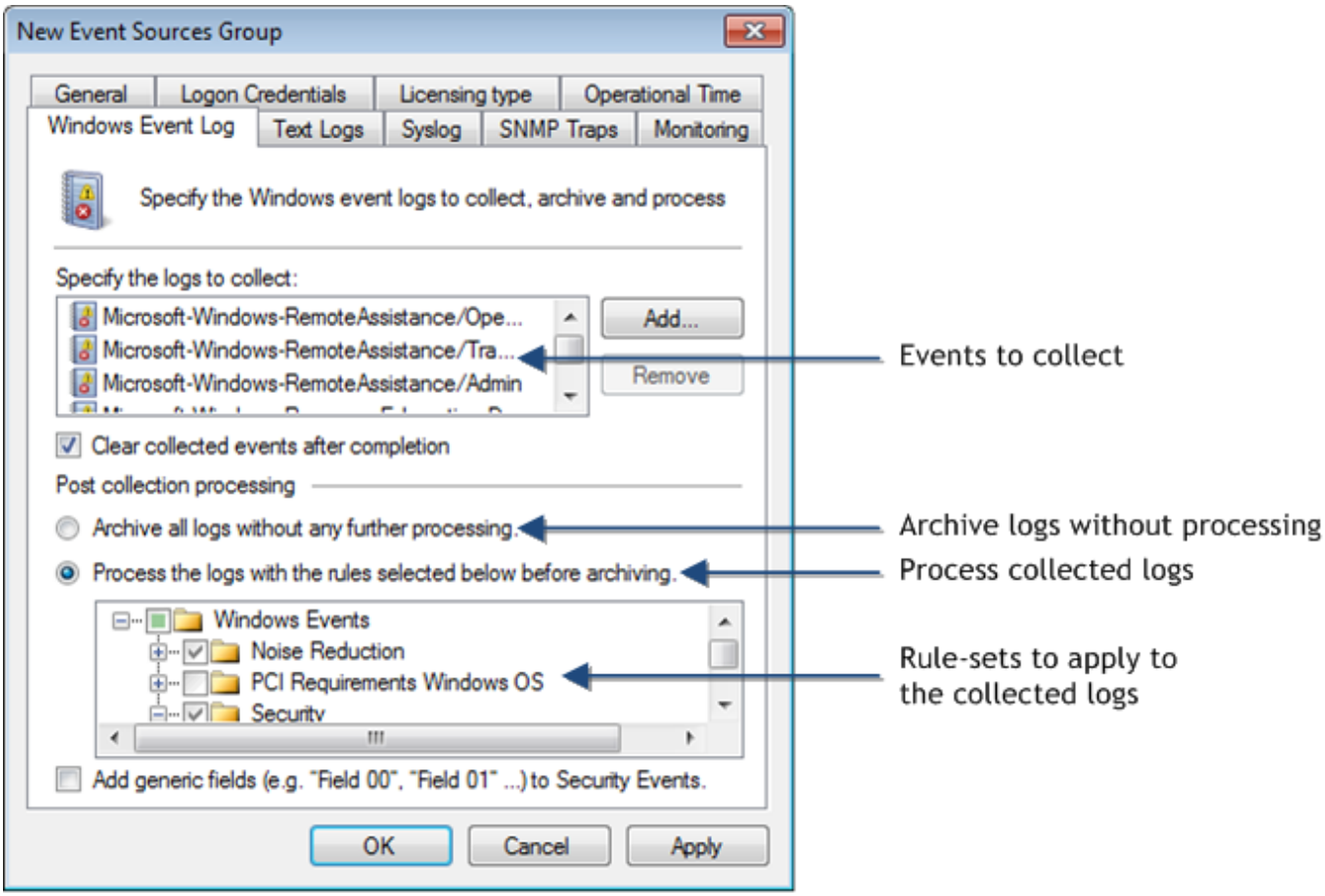
Windows® events are organized into specific log categories; by default computers running on Windows® NT or higher, record errors, warnings and information events in three logs namely **Security**, **Application** and **System logs**.

Computers that have more specialized roles on the network such as Domain Controllers, and DNS Servers have additional event log categories.

As a minimum, Windows® Operating Systems record events in the following logs:

Table 36: Windows® Event Logs collected by GFI EventsManager

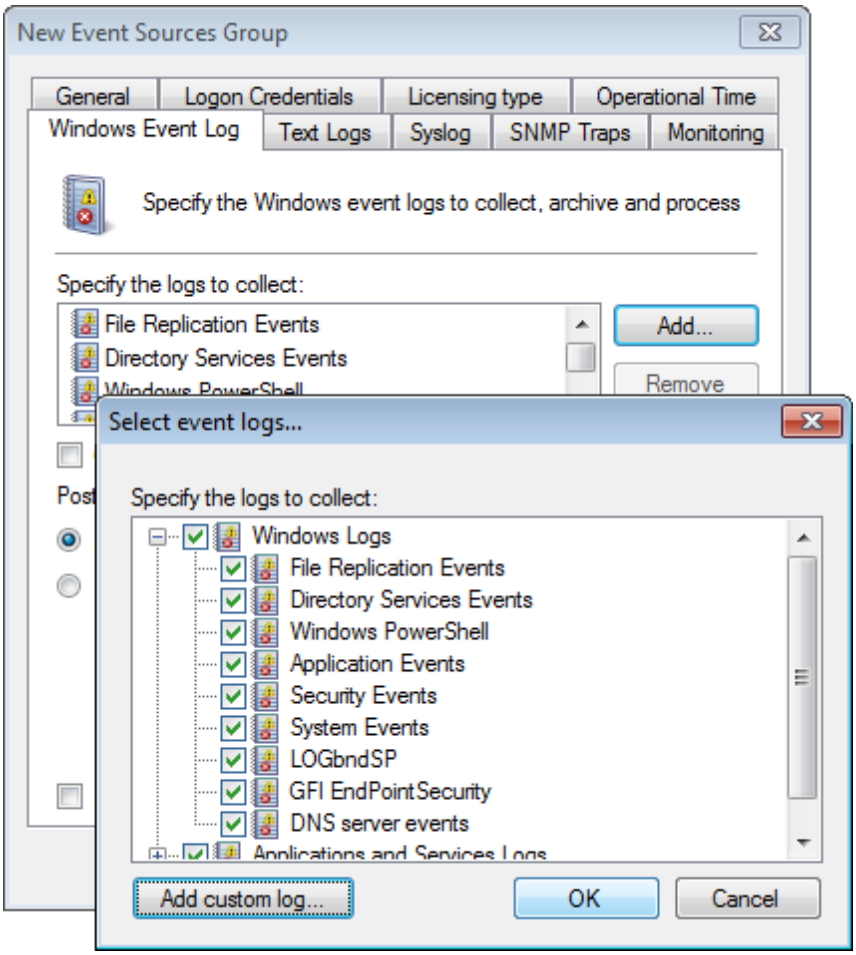
Log Type	Description
Security event log	This log contains security related events through which you can audit successful or attempted security breaches. Typical events found in the Security Events log include valid and invalid logon attempts.
Application event log	This log contains events recorded by software applications/programs such as file errors.
System event log	This log contains events logged by operating system components such as failures to load device drivers.
Directory service log	This log contains events generated by the Active Directory including successful or failed attempts to make to update the Active Directory database.
File Replication service log	This log contains events recorded by the Windows® File Replication service. These including file replication failures and events that occur while domain controllers are being updated with information about Sysvol.
DNS server log	This log contains events associated with the process of resolving DNS names to IP addresses.
Application and Services Logs	These logs contain events associated with Windows® VISTA and the relative services/functionality it offers.



Screenshot 69: Computer group properties: Configuring Windows® Event Logs parameters

To configure Windows® Event Log collection and processing parameters:

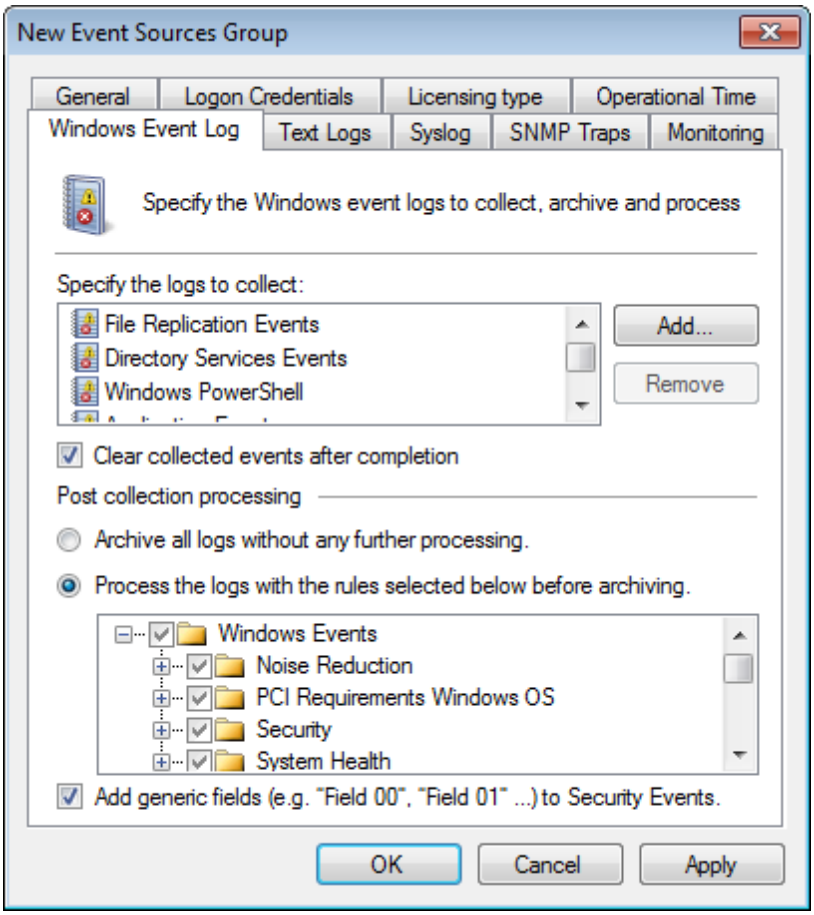
1. From **Configuration** tab **>** **Event Sources**, right-click an event source or group and select **Properties**.



Screenshot 70: Selecting event logs to collect

2. Click **Windows Event Log** tab > **Add...** to select the logs you want to collect. Expand **Windows Logs** and/or **Applications and Services Logs** and select from the list of available logs.

3. (Optional) Click **Add custom log...** and key in a unique name for the unlisted event log.



Screenshot 71: Configuring Windows Event Log Processing parameters

4. Select **Clear collected events after completion** to clear the collected events from the respective event source.

5. Select **Archive events in database** to archive collected events without applying events processing rules.

6. Select **Process using these rule sets** and select the rule sets you want to run against the collected events.

7. Select **Add generic fields** to add extended fields to the database. Extended fields contain data from event descriptions and are added by a common name (example: "Field01", "Custom field name").

8. Click **Apply** and **OK**.

Important

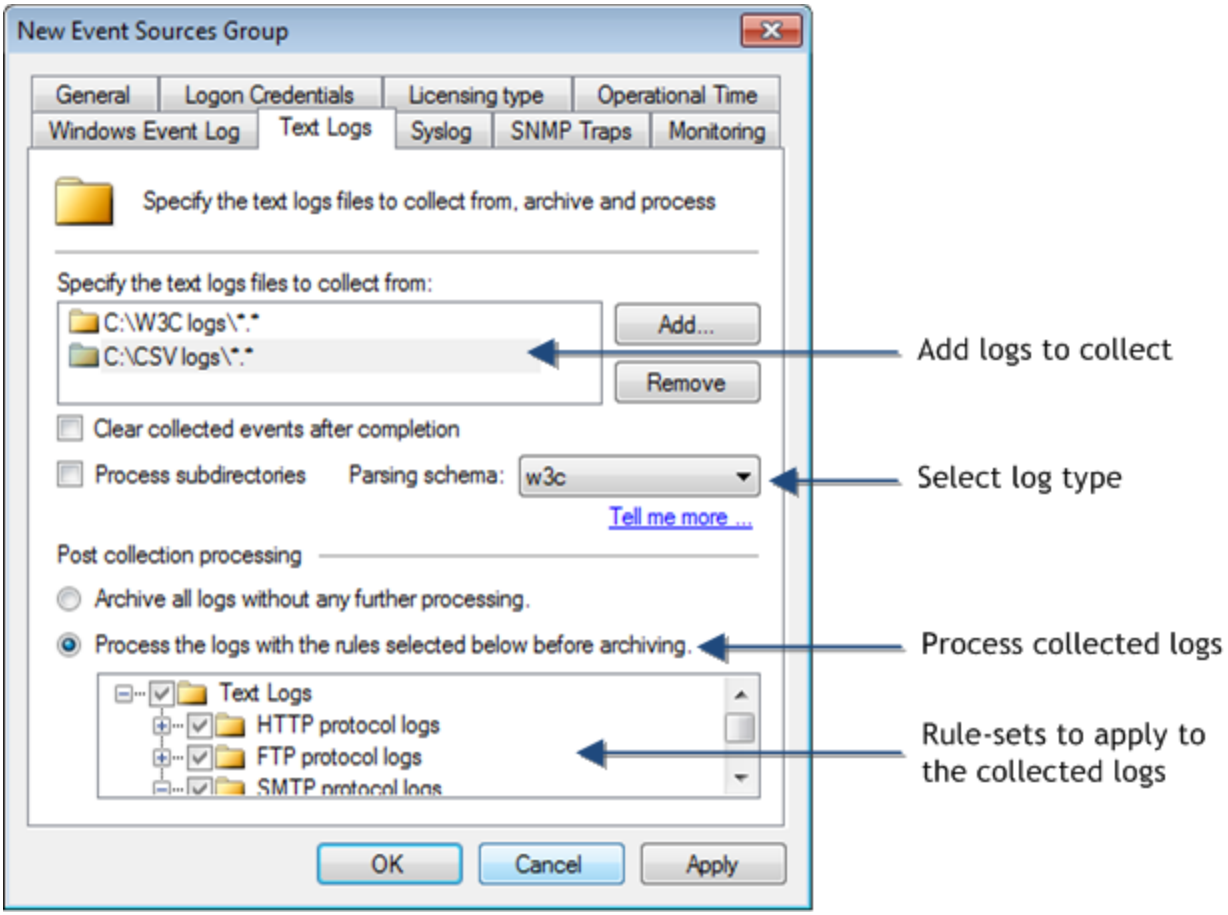
Deleting event logs without archiving may lead to legal compliance penalties.

5.2 Collecting Text logs

Text Logs are other log formats supported by GFI EventsManager. W3C logs are text-based flat files containing various event details delimited by special characters.

The W3C log format is most commonly used by hardware systems (Example: servers and appliances) which have Internet specific roles. Microsoft® Internet Information Server (IIS) service and Apache web servers for example, can collect web related events such as web logs, in the form of W3C formatted text files.

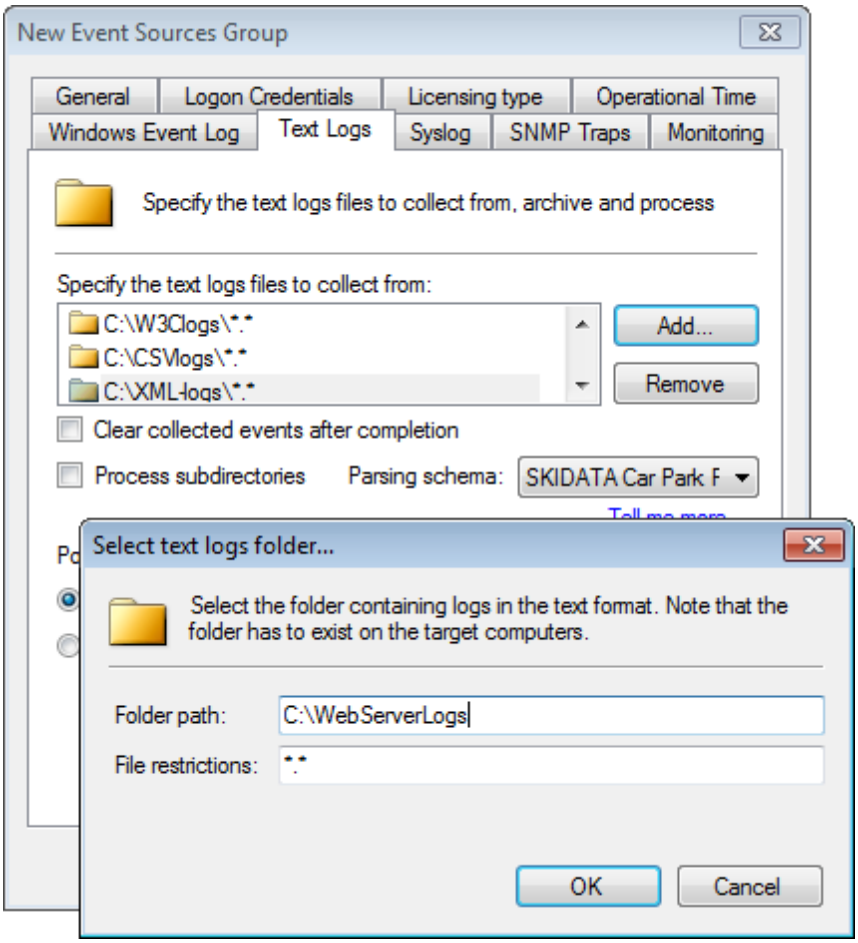
In GFI EventsManager, the configuration process of W3C log parameters is identical to that performed for Windows® event processing, with one exception. Unlike Windows® Event Logs, there is no standard which dictates a specific or centralized folder location where W3C log files are stored on disk. Therefore, in order to collect W3C logs, you must specify the complete path to these text-based log files.



Screenshot 72: Text logs options

To collect Text logs:

1. From **Configuration** tab **>** **Event Sources**, right-click an event source or group and select **Properties**.



Screenshot 73: Adding folders containing Text Logs

2. Click **Text Logs** tab > **Add...** to add folder paths containing Text Logs.

3. From the **Select text logs folder...** dialog, key in the path to the folder containing the text logs files and Click **OK**.

4. Select **Clear collected events after completion** to clear the collected events from the respective event source.

5. Select **Process subdirectories** to recursively scan the specified path that contains the text logs.

6. From **Parsing schema** drop-down menu, select the schema in which Text Logs are interpreted. Select from:

- W3C
- CSV
- DHCP
- XML
- SAP Logs
- ESM Logs
- SKI Data Car Park Payments.

7. Select **Archive events in database** to archive collected events without applying events processing rules.

8. Select **Process using these rule sets** and select the rule sets you want to run against the collected events.

9. Click **Apply** and **OK**.

> **Important**
>
> Deleting event logs without archiving may lead to legal compliance penalties.

5.3 Collecting Syslogs

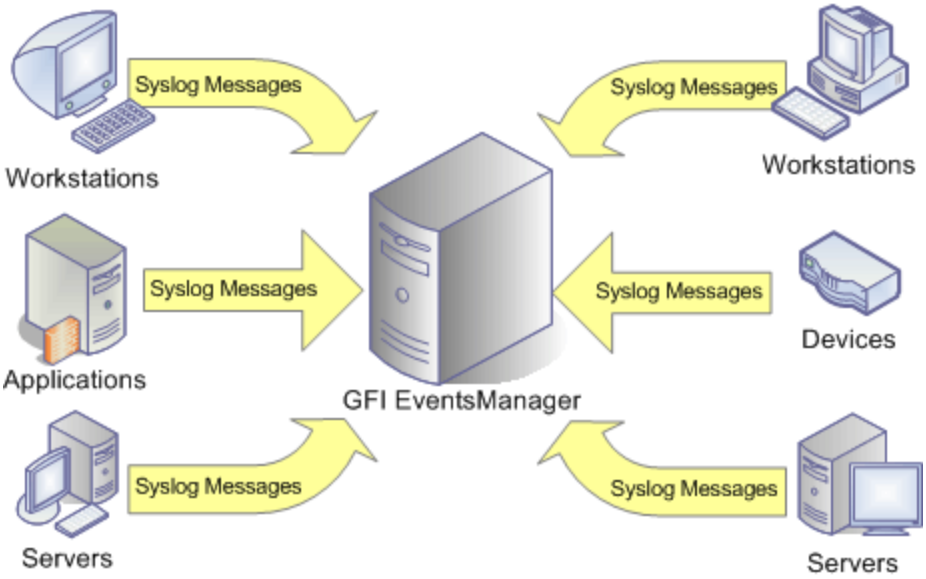
Syslog is a data logging service that is most commonly used by Linux and UNIX based systems. The concept behind Syslogs is that the logging of events and information is entirely handled by a dedicated server called 'Syslog Server'.

Unlike Windows® and Text log based systems, Syslog enabled devices send events in the form of data messages (technically known as 'Syslog Messages') to a Syslog server that interprets and manages message and saves the data in a log file.

In order to process Syslog messages, GFI EventsManager ships with a built-in Syslog Server. This Syslog server will automatically collect, in real-time, all Syslog messages/events sent by Syslog sources and pass them on to the event processing engine. Out-of-the-box, GFI EventsManager supports events generated by various network devices manufactured by leading providers including Cisco and Juniper.

> **Note**
>
> For more information about supported devices visit the following KBASE article:
> http://go.gfi.com/?pageid=esm_syslog_snmp_support

> **Note**
>
> A built-in buffer allows the Syslog server to collect, queue and forward up to 30 Syslog messages at a time. Buffered logs are by default passed on to the event processing engine as soon as the buffer fills up or at one minute intervals; whichever comes first.



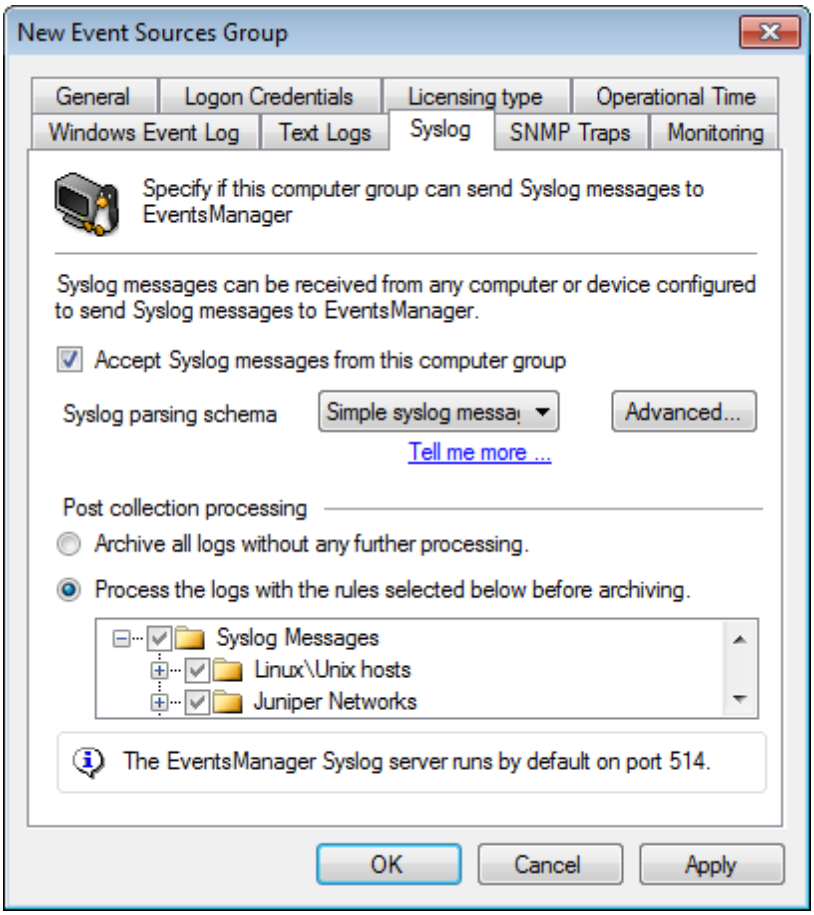
Screenshot 74: Syslog messages must be directed to the computer running GFI EventsManager

Important

Before you start collecting Syslogs, every Syslog event source (workstations, servers and/or network devices) must be configured to send their Syslog Messages to the computer name or IP where GFI EventsManager is installed.

To collect Syslogs:

1. From **Configuration** tab **> Event Sources**, right-click an event source or group and select **Properties**.



Screenshot 75: Collecting Syslogs - Syslogs options

2. Click **Syslog** tab and select **Accept Syslog messages to EventsManager** to enable the collection of Syslogs from that event source/event source group.

3. From the **Syslog parsing schema** drop-down, select the method that GFI EventsManager Syslog Server interprets Syslog Messages from network devices. Select from:

- Simple Syslog message
- Standard Linux message
- Juniper Network Firewall
- Cisco ASA.

4. Click **Advanced…** to use custom windows code page. Specify the code and click **OK**.

> **Note**
>
> Windows® code page is used to encode international characters to ASCII strings. Since Syslog is not Unicode compliant, GFI EventsManager uses a code page to decode the events. This is only applicable if GFI EventsManager is installed on a machine using a different language than the monitored machines. For more information, refer to: http://go.gfi.com/?pageid=esm_code_page

5. Select **Archive events in database** to archive collected events without applying events processing rules.

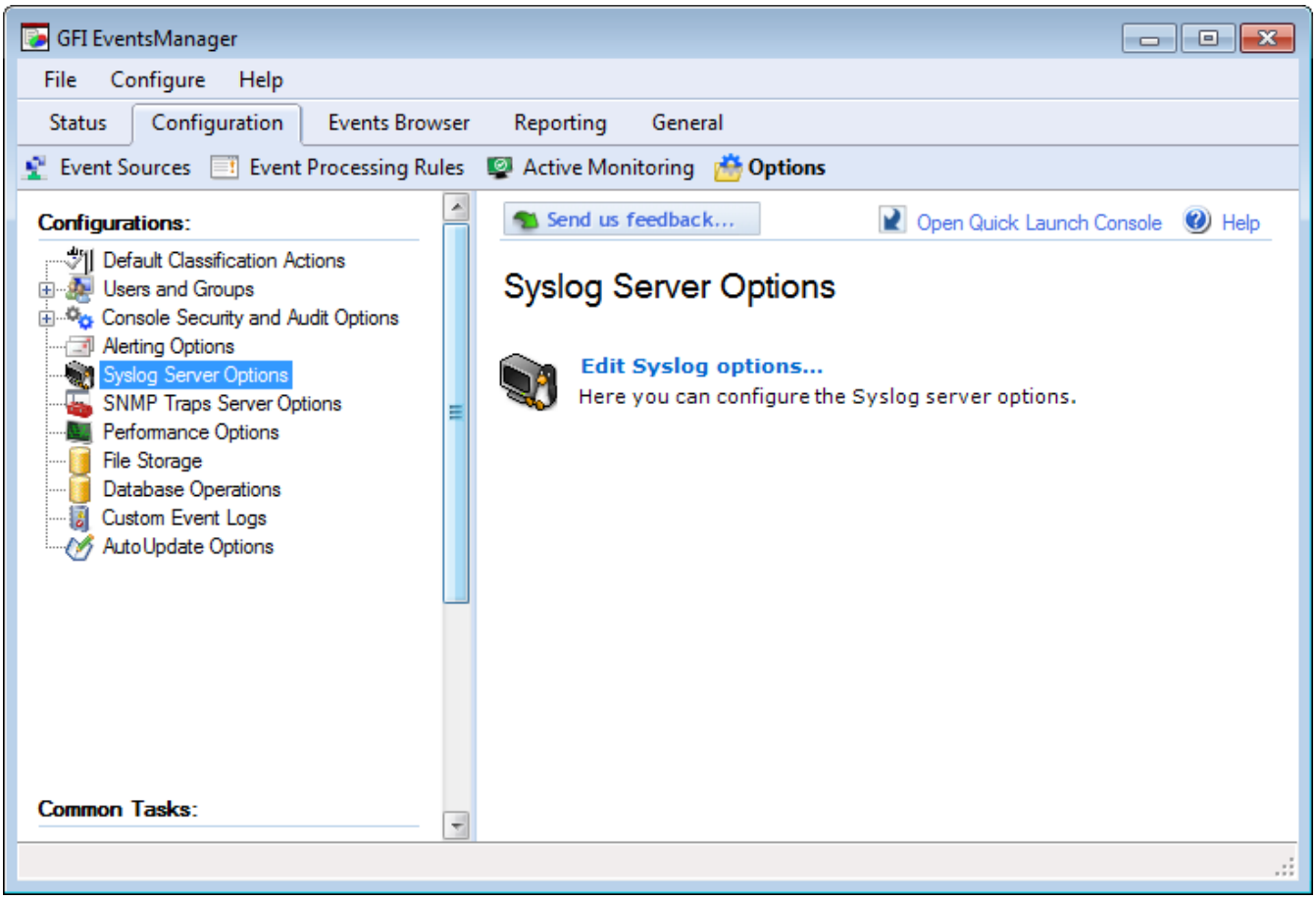
6. Select **Process using these rule sets** and select the rule sets you want to run against the collected events.

7. Click **Apply** and **OK**.

> **Note**
>
> The GFI EventsManager Syslog server is by default configured to listen for Syslog messages on port **514**. For more information refer to Configuring the Syslog server communications port.

> **Important**
>
> Deleting event logs without archiving may lead to legal compliance penalties.

5.3.1 Configuring the Syslog server communications port

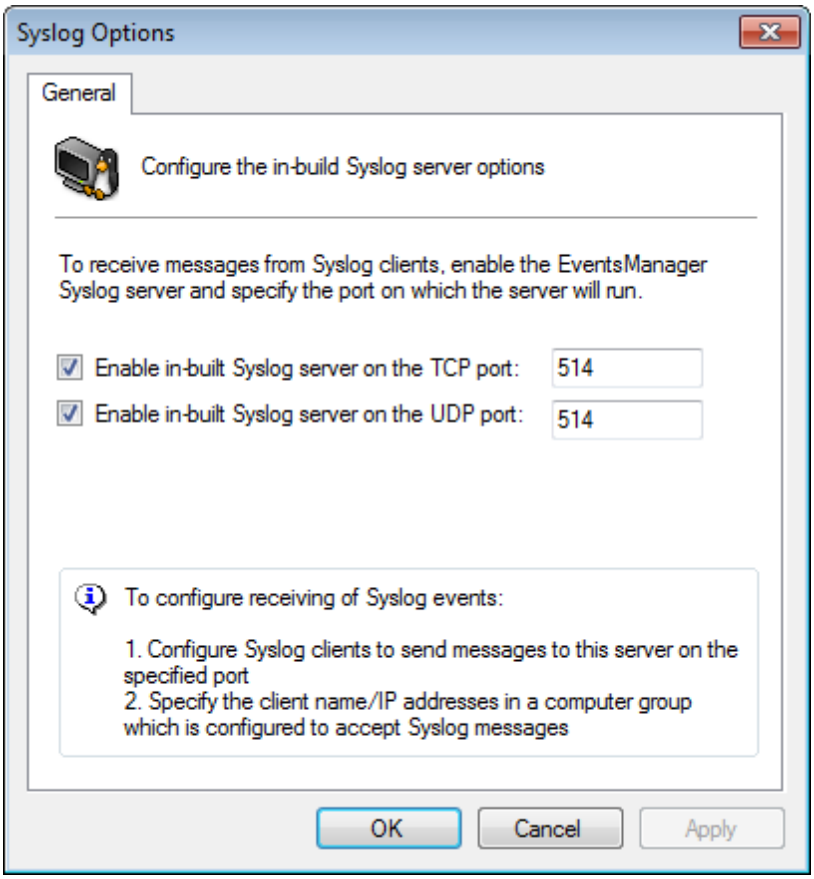


Screenshot 76: Configuring Syslog Server communication port

To change the default Syslog ports settings:

1. Click **Configuration** tab > **Options**.

2. Right-click **Syslog Server Options** and select **Edit Syslog options...**


Syslog Options
General
Configure the in-build Syslog server options
To receive messages from Syslog clients, enable the EventsManager Syslog server and specify the port on which the server will run.
Enable in-built Syslog server on the TCP port:
514
Enable in-built Syslog server on the UDP port:
514
To configure receiving of Syslog events:
1. Configure Syslog clients to send messages to this server on the specified port
2. Specify the client name/IP addresses in a computer group which is configured to accept Syslog messages
OK
Cancel
Apply

Screenshot 77: Syslog server options

4. Select **Enable in-built Syslog server on TCP port:** and specify the TCP port on which GFI EventsManager will receive/listen for Syslog messages.

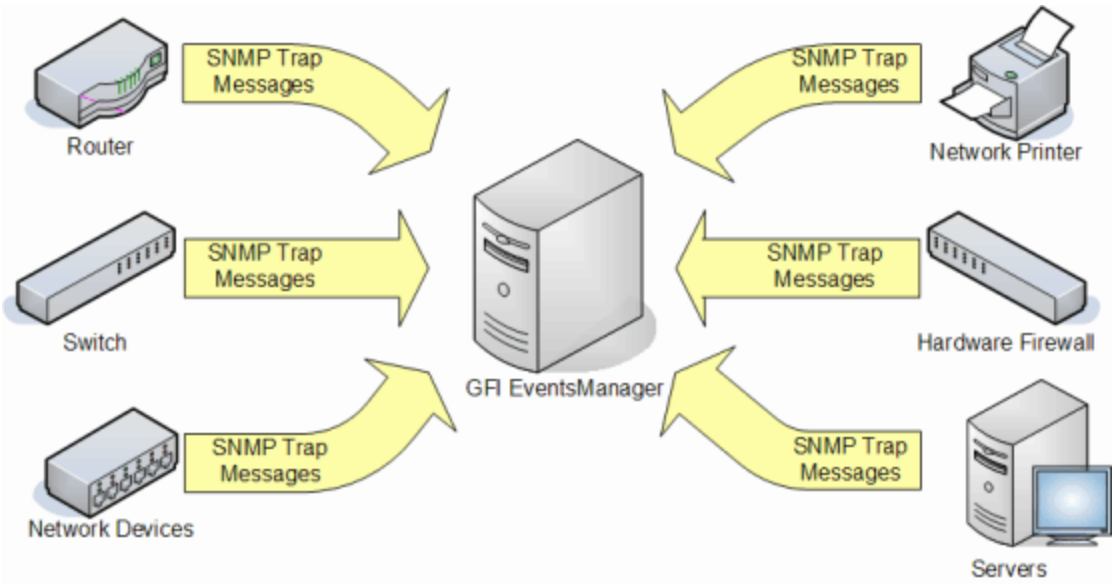
5. Select **Enable in-built Syslog server on UDP port:** and specify the UDP port on which GFI EventsManager will receive/listen for Syslog messages.

6. Click **Apply** and **OK**.

> **Note**
>
> When configuring Syslog server port settings, make sure that the configured port is not already in use by other installed applications. This may affect the delivery of Syslog messages to GFI EventsManager.

5.4 Collecting SNMP Traps Messages

SNMP is a data logging service that enables networked devices to log events and information through data messages (technically known as SNMP Traps). SNMP messaging technology is similar in concept to Syslogs - where unlike Windows® and Text logs based environments, devices that generate SNMP messages do not record events data in local logs. Instead events information is sent in the form of data messages to an SNMP Trap Server which manages and saves SNMP message data in a local (centralized) log file.



Screenshot 78: SNMP Trap messages must be directed to the computer running GFI EventsManager

Note

GFI EventsManager natively supports an extensive list of SNMP devices and Management Information Bases (MIBs). For a full list of supported devices, view the following KBASE article: http://go.gfi.com/?pageid=esm_syslog_snmp_support

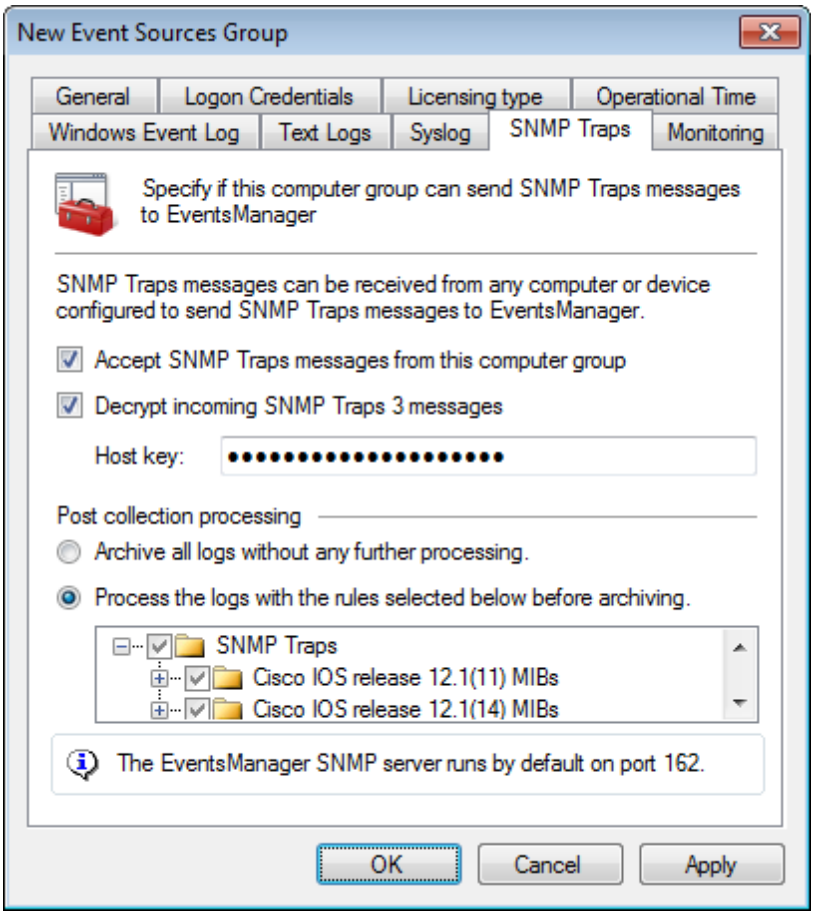
GFI EventsManager includes a dedicated SNMP Trap Server through which SNMP Traps are handled. A built-in buffer allows the SNMP Trap Server to collect, queue and forward up to 30 SNMP Trap at a time. Buffered logs are by default passed on to the event processing engine as soon as the buffer fills up or at one minute intervals; whichever comes first.

Important

Before you start collecting SNMP Traps messages, every SNMP event source (workstations, servers and/or network devices) must be configured to send their SNMP Traps Messages to the computer name or IP where GFI EventsManager is installed.

To collect SNMP Traps:

1. From **Configuration** tab > **Event Sources**, right-click an event source or group and select **Properties**.


New Event Sources Group
General
Logon Credentials
Licensing type
Operational Time
Windows Event Log
Text Logs
Syslog
SNMP Traps
Monitoring
Specify if this computer group can send SNMP Traps messages to EventsManager
SNMP Traps messages can be received from any computer or device configured to send SNMP Traps messages to EventsManager.
Accept SNMP Traps messages from this computer group
Decrypt incoming SNMP Traps 3 messages
Host key:
Post collection processing
Archive all logs without any further processing.
Process the logs with the rules selected below before archiving.
SNMP Traps
Cisco IOS release 12.1(11) MIBs
Cisco IOS release 12.1(14) MIBs
The EventsManager SNMP server runs by default on port 162.
OK
Cancel
Apply

Screenshot 79: Collecting SNMP Traps

2. Click **SNMP Traps** tab and select **Accept SNMP Traps messages from this event source** to enable the collection of SNMP Traps.

3. Select **Decrypt incoming SNMP Traps 3 messages** and specify the security key in the **Host key** text box.

4. Select **Archive events in database** to archive collected events without applying events processing rules.

5. Select **Process using these rule sets** and select the rule sets you want to run against the collected events.

6. Click **Apply** and **OK**.

Note

The GFI EventsManager SNMP Trap Server is by default configured to listen for SNMP Trap messages on port **162**. For more information refer to Configuring the SNMP Traps server.

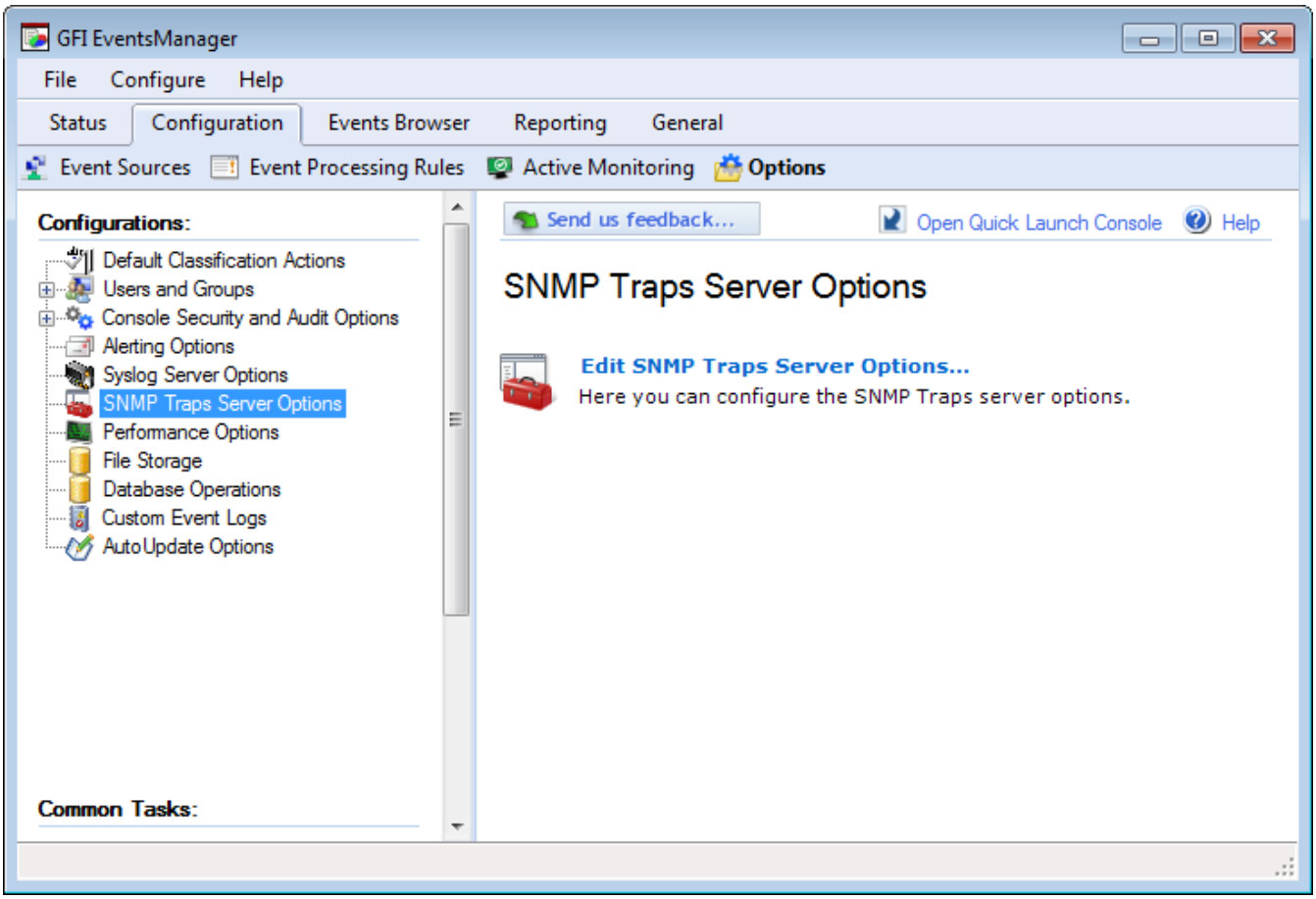
Note

The built in SNMP Trap Server supports SNMP version 3 Traps with encryption. For encrypted SNMP messages the encryption host key must be provided in the decrypt incoming SNMP Traps 3 message field.

Important

Deleting event logs without archiving may lead to legal compliance penalties.

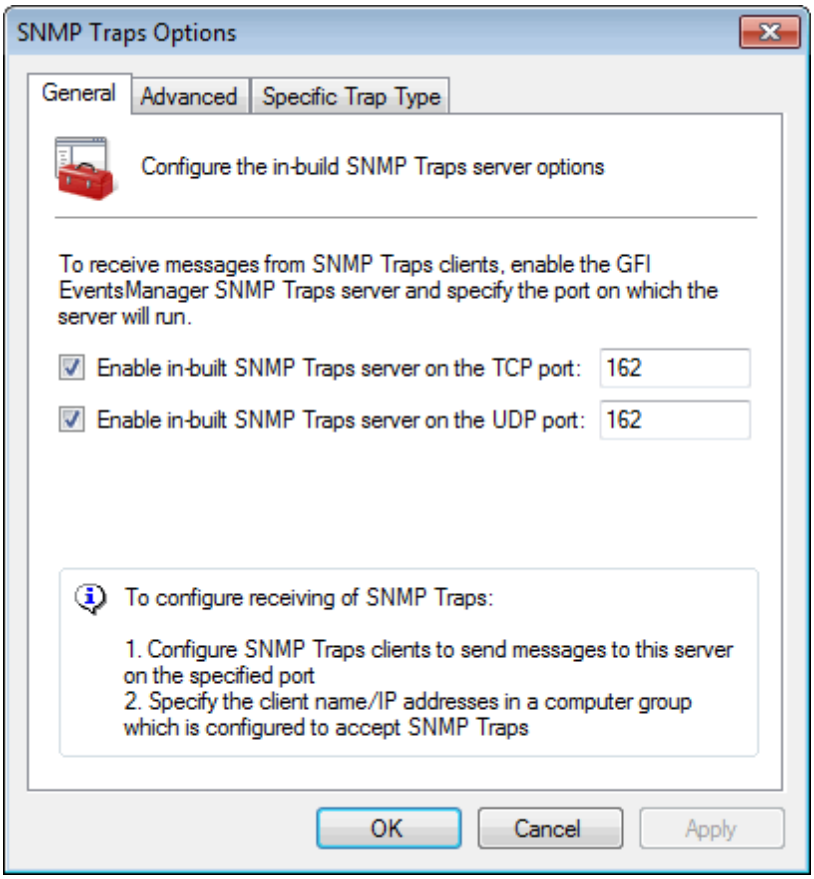
5.4.1 Configuring the SNMP Trap server



Screenshot 80: Configuring SNMP Traps

To change the default SNMP Trap Server settings:

1. Click **Configuration** tab > **Options**.
2. Right-click **SNMP Traps Options** and select **Edit SNMP Traps options…**


SNMP Traps Options
General
Advanced
Specific Trap Type
Configure the in-build SNMP Traps server options
To receive messages from SNMP Traps clients, enable the GFI EventsManager SNMP Traps server and specify the port on which the server will run.
Enable in-built SNMP Traps server on the TCP port:
162
Enable in-built SNMP Traps server on the UDP port:
162
To configure receiving of SNMP Traps:
1. Configure SNMP Traps clients to send messages to this server on the specified port
2. Specify the client name/IP addresses in a computer group which is configured to accept SNMP Traps
OK
Cancel
Apply

Screenshot 81: SNMP Traps options

3. Enable the required TCP/UDP SNMP server. Specify the TCP/UDP port on which GFI EventsManager will listen for SNMP messages.

4. Click **Advanced** tab to add, edit or remove SNMP Trap object identifiers (OIDs).

5. Click **Specific Trap Type** tab to add, edit or remove trap types.

6. Click **Apply** and **OK**.

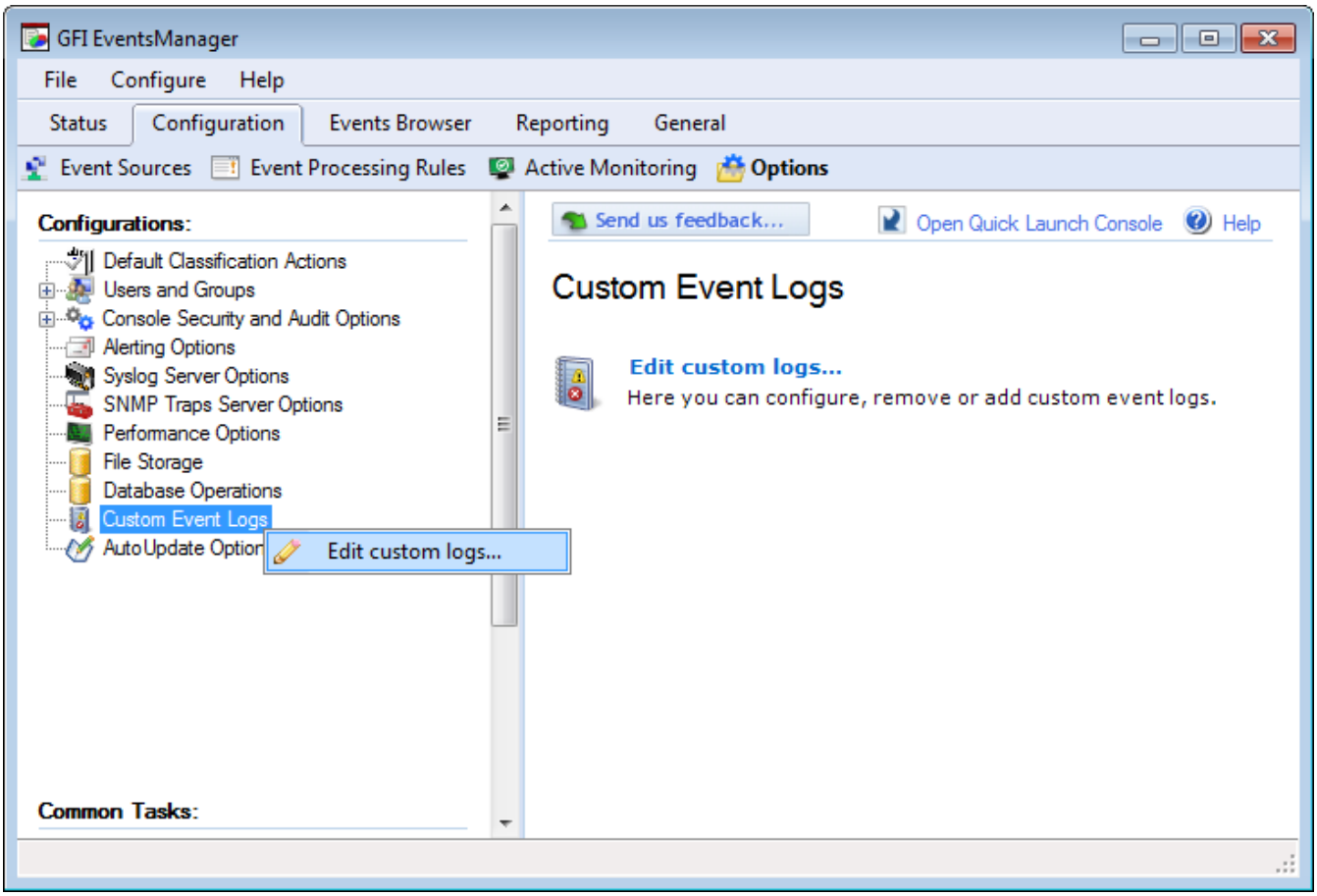
> **Note**
>
> When configuring SNMP Trap Server port settings, make sure that the configured TCP or UDP port is not already in use by other installed applications. This may affect the delivery of SNMP Trap messages to GFI EventsManager.

5.5 Collecting custom logs

GFI EventsManager is configured to collect and process standard event logs. However, GFI EventsManager can also be configured to manage events recorded in third party application logs such as anti-virus logs, software firewall logs and other security software.

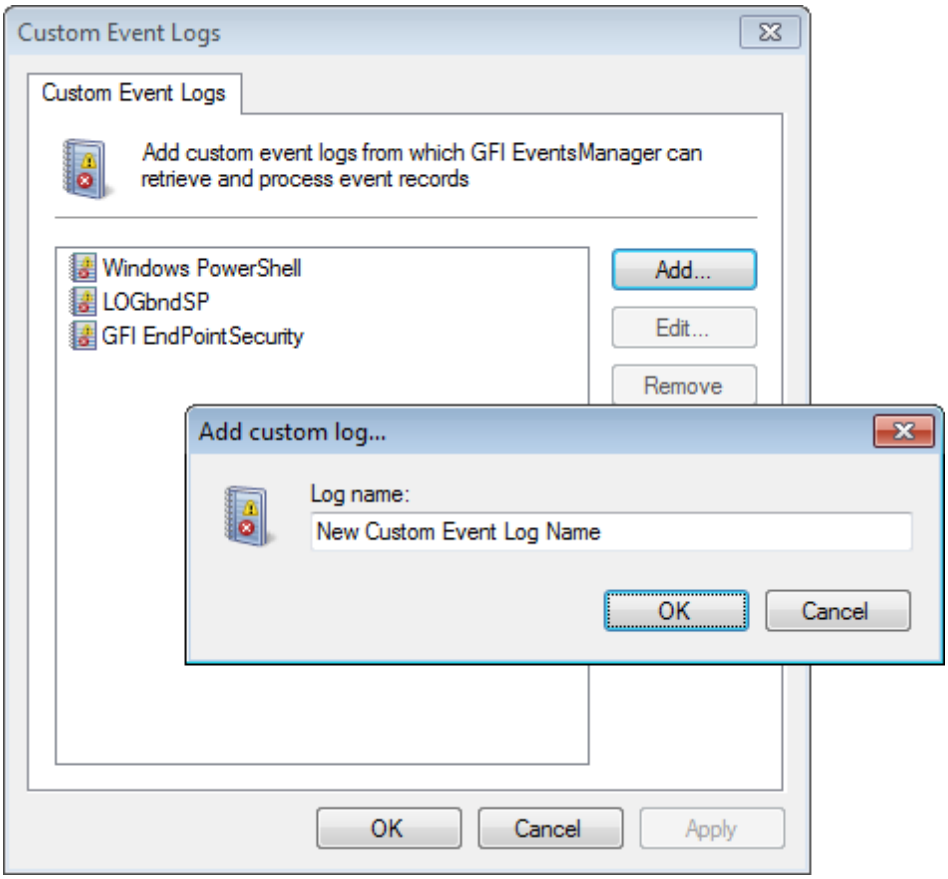
To configure custom events:

1. Click **Configuration** tab > **Options**.



Screenshot 82: Custom event logs setup

2. From **Configurations**, right-click **Custom Event Logs** and select **Edit custom logs...**



Screenshot 83: Custom event logs dialog

3. Click **Add…** button and specify the name of your custom event log.

4. Click **OK**.

5. (Optional) Click **Edit** to rename the selected custom event, or click **Remove** to delete the selected custom event.

6. Click **Apply** and **OK**.

5.6 Collecting GFI LanGuard event logs

GFI EventsManager enables you to monitor events generated by GFI LanGuard. GFI LanGuard is a network vulnerability scanner that audits your network for weaknesses that can be exploited by users for malicious purposes. During network audits, GFI LanGuard creates events in the '**Application Log**' of the machine where it is installed.

For each machine scanned by GFI LanGuard, an 'Application log' entry having '**Event ID: 0**' and '**Source**' set as **GFI LanGuard** will be generated. These events denote network vulnerability information extracted from scanned computers including:

Table 37: Information gathered by GFI LanGuard

Gathered Information	Description
Threat level	Gather information about the overall network threat level. This rating is generated through an extensive algorithm after GFI LanGuard audits the network.
Missing patches and service packs	Find out which machines have missing updates and which updates need to be installed to strengthen the security level.
Open ports	Discover any unwanted open TCP and/or UDP ports.

Gathered Information	Description
Antivirus operational and malware definition status	GFI LanGuard is able to check if your virus database definitions are up to date. If it is not, you will be alerted and GFI LanGuard will attempt to update it.
Applications detected on scanned targets	GFI LanGuard enumerates applications installed on scan targets. You can create an inventory of wanted and/or unwanted applications and configure GFI LanGuard to automatically uninstall applications categorized as unwanted.

Note

For more information about GFI LanGuard, refer to http://www.gfi.com/network-security-vulnerability-scanner.

Note

GFI EventsManager can process events generated by GFI LanGuard version 9.5 or later.

5.6.1 How to enable GFI LanGuard event logging?

There are two key steps needed to enable event log integration between GFI LanGuard and GFI EventsManager:

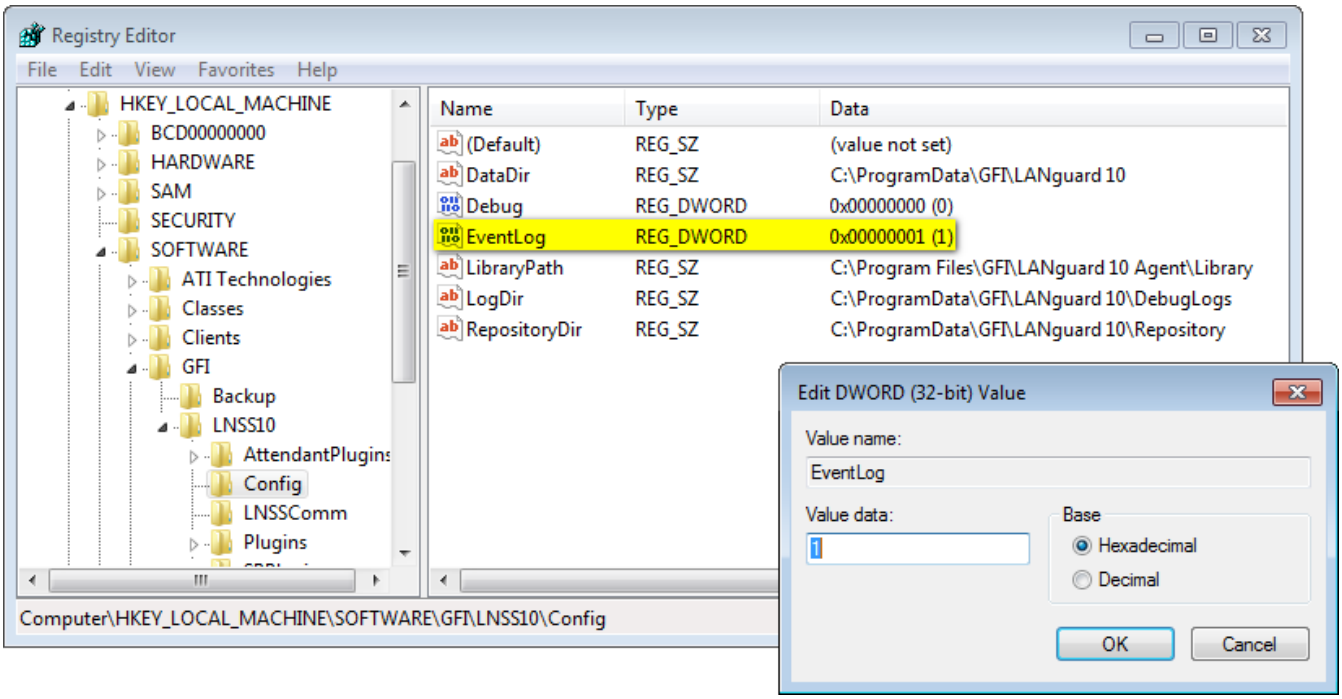
- Step 1: Enable logging
- Step 2: Configure GFI EventsManager to collect Application Logs

Step 1: Enable GFI LanGuard logging

To enable GFI LanGuard to output event logs on completion of system audits:

1. Add the machine where GFI LanGuard is installed as an event source.

2. Click **Start > Run** and key in **regedit**. Press **Enter**.



Screenshot 84: Enabling GFI LanGuard logging through the registry

3. Go to the following registry key and edit the value to enable event logging:

» **Windows® x86 platforms:**

- `HKEY_LOCAL_MACHINE\SOFTWARE\GFI\LNSS[n]\Config`
- Set value of **REG_DWORD EventLog** to **1**

» **Windows® x64 platforms:**

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GFI\LNSS[n]\Config`
- Set value of **REG_DWORD EventLog** to **1**

Important

[n] is the major version number of GFI LanGuard.

Example: HKEY_LOCAL_MACHINE\SOFTWARE\GFI\LNSS**9**\Config\EventLog = 1(dword)

Note

To stop GFI LanGuard from generating 'Application Log' entries, remove the registry value described above or change the registry value to **0**.

Step 2: Configure GFI EventsManager to collect Application logs

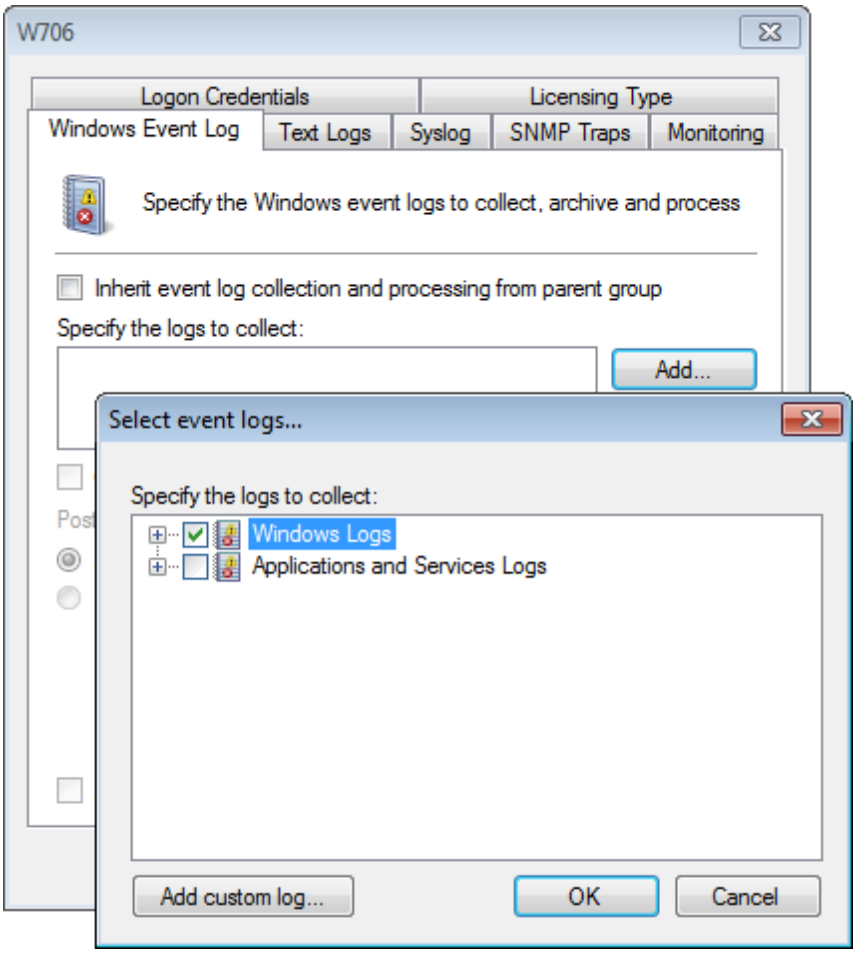
GFI LanGuard outputs windows event logs to the 'Application Log' category. Ensure that the collection of Application logs is enabled on the GFI LanGuard event source.

To enable processing of GFI LanGuard events:

1. Open GFI EventsManager Management Console.

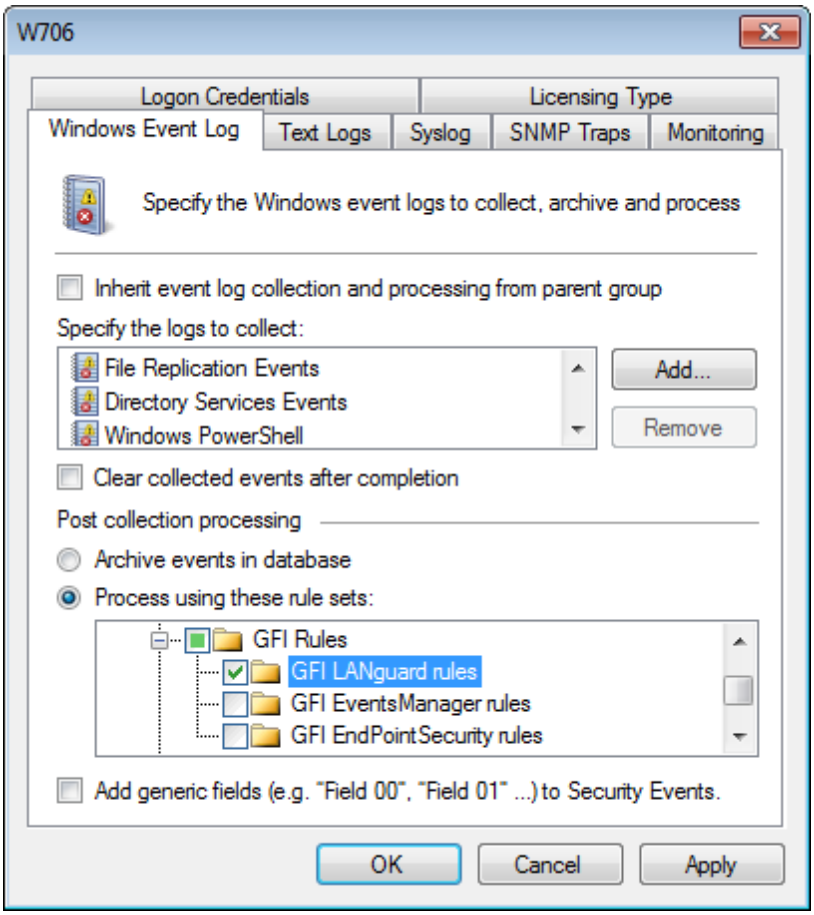
2. Click **Configuration** tab > **Event Sources**.

3. Right-click on the GFI LanGuard event source and select **Properties.**



Screenshot 85: Add Windows® Application logs

4. From **Windows® Event Log** tab, click **Add** and select **Windows® Logs**. Click **OK**.



Screenshot 86: Add GFI LanGuard rules

5. Select **Process using these rule sets**. Expand **Windows Events > GFI Rules** node and select **GFI LanGuard rules**.

6. Click **OK**.

> **Note**
>
> GFI EventsManager has built-in processing rules for GFI LanGuardevents that are enabled by default. To monitor events generated by GFI LanGuard, select **Status** tab > **General** and locate the **Critical and High Importance Events** section.

> **Note**
>
> To configure GFI LanGuard event processing rules, click **Configuration** tab > **Event Processing Rules**. From the left pane select **GFI Rules > GFI LanGuardrules**. For more information refer to Events Processing Rules.

Testing and troubleshooting

To check if GFI LanGuard events are being generated:

1. Open GFI LanGuard and run a security audit scan on the localhost.

2. When the scan finishes, open **Event Viewer** from **Start > Run** and key in **eventvwr**. Press **Enter**.

3. Go to Event Viewer (local) Windows Logs Application.

4. Once the stored events are loaded, search for an entry with:

- Source: GFI LanGuard
- Event ID: 0.

In case the event log is not created, typically the GFI LanGuard scan was already initiated once the registry key to output event logs was modified. Re-run the scan. Alternatively ensure that the registry value was created in the right location as the location for x86 platforms is different from that of x64 platforms.

5.7 Collecting GFI EndPointSecurity events

GFI EndPointSecurity enables you to maintain data integrity by preventing unauthorized access, and, the transfer of content to and from the following devices or connection ports:

Table 38: GFI EndPointSecurity supported devices

Device	Example
USB Ports	Flash/Memory card readers and pen drives.
Firewire ports	Digital cameras and Fire-wire card readers.
Wireless devices	Bluetooth and Infrared dongles
Floppy disk drives	Internal and external (USB) floppy drives.
Optical drives	CD, DVD and Blu-ray discs.
Magneto Optical drives	Internal and external (USB) drives.
Removable storage	USB hard-disk drives.
Other drives such as Zip drives and tape drives	Internal or External (USB/Serial/Parallel) drives.

Note

For more information about GFI EndPointSecurity, refer to http://www.gfi.com/endpointsecurity.

Enable GFI EndPointSecurity logging

By default, GFI EndPointSecurity generates logs with information about:

- The GFI EndPointSecurity service
- Devices connected and disconnected on your network
- Access allowed or denied by GFI EndPointSecurity to users.

To configure logging options in GFI EndPointSecurity:

1. From the machine running GFI EndPointSecurity machine, launch GFI EndPointSecurity Management Console.

2. Click **Configuration** tab > **Protection Policies**.

3. From the left pane, select the protection policy and click **Set Logging Options**.

4. Customize the settings available in Logging Option dialog.

Note

For more information on how to configure GFI EndPointSecurity logging options, refer to the GFI EndPointSecurity documentation available from http://www.gfi.com/products/gfi-endpointsecurity/manual.

Monitor GFI EndPointSecurity Events

GFI EventsManager has built-in processing rules for GFI EndPointSecurity events that are enabled by default. To monitor events generated by GFI EndPointSecurity, select **Status** tab > **General** and locate the **Critical and High Importance Events** section.

To configure GFI EndPointSecurity event processing rules, click **Configuration** tab > **Event Processing Rules**. For more information refer to Events Processing Rules.

6 Browsing Stored Events

This chapter provides you with information about using the Events Browser. The Events Browser is equipped with tools for event analysis and forensic investigation. It also enables you to easily browse through multiple events databases as well as export events to encrypted databases for legal compliance purposes.

Topics in this chapter:

6.1 Navigating the Events Browser 123

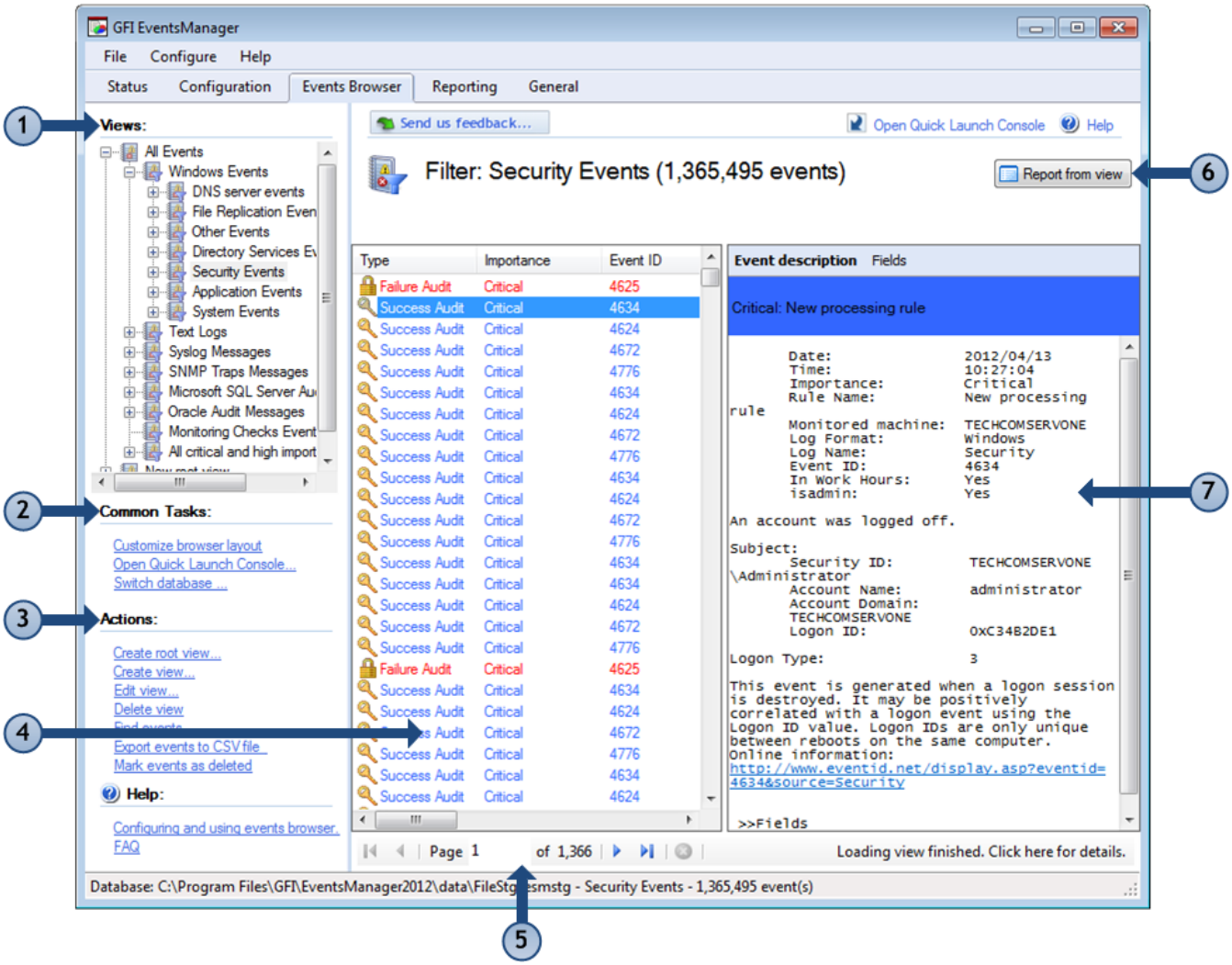
6.2 Using the Events Browser 124

6.3 Managing Events Browser views 127

6.4 Customizing Events Browser layout 130

6.5 Browsing events from different databases 132

6.1 Navigating the Events Browser



Screenshot 87: Events Browser

The Events Browser is made up of the following sections:

Table 39: Navigating the Events Browser

	Section	Description
1	**Views**	The **Views** section includes a wide range of predefined views. Use this section to view specific logs such as Windows® Event Logs, Text Logs, SQL Server® audits and more.
2	**Common Tasks**	**Common Tasks** enable you to customize the look of the Events Browser and switch database to view exported and/or archived event logs.
3	**Actions**	Use the **Actions** section to run common functions related to analyzing event logs. This enables you create or edit custom views, export events for further analysis and more.
4	**Events**	The **Events** section is used to browse through the events categorized under the selected view (from section 1).
5	**Navigation controls**	Use the navigation controls to browse through collected events.
6	**Reporting**	The **Report from view** option enables you to generate graphical and statistical reports based on the selected view (from section 1).
7	**Event Description Pane**	The **Events Description Pane** provides an extensive breakdown of the selected event (from section 4). Use this section to analyze the event details and find out when the event was generated, what was the cause and by whom it was generated. The header color coding enables you to quickly identify the severity of the event. The description section enables you to switch between two views: » **General** - Contains event information in the legacy format that was standard for pre-Microsoft® Windows® Vista event logs. » **Fields** - Contains a list of event information categorized by fields. The link provided in the event description gives you access to: » A more detailed description of the event » Information and links that explain what causes this type of event » Hints and tips on how to possibly solve any existing issues.

6.2 Using the Events Browser

Event analysis is a demanding task; GFI EventsManager is equipped with specialized tools that simplify this process. Use the Events Browser for forensic analysis of events. All events accessible through the Events Browser are organized by log type in the **Views** section. The following sections describe how to use the Events Browser to manage your events:

- Exporting events to CSV
- Creating reports from events browser views
- Deleting events
- Searching stored events
- Identifying rules using the rule finder tool

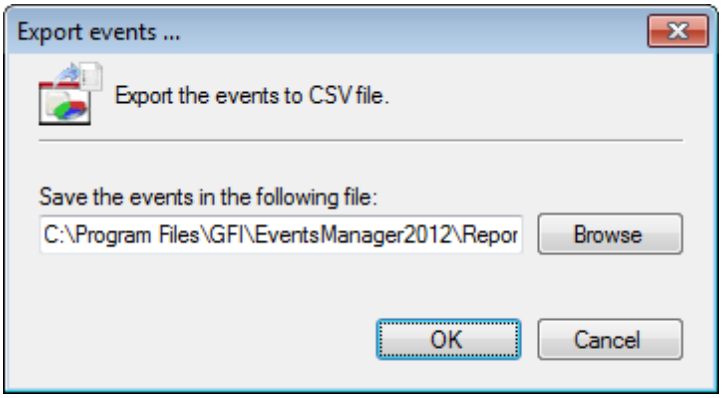
6.2.1 Exporting events to CSV

GFI EventsManager enables you to export event data to CSV files directly from Events Browser. This is extremely convenient especially when further processing of event data is required. This includes:

- Distribution of key event data via email
- Running automated scripts that convert CSV exported events data to HTML for upload on web/company intranet
- Generation of graphical management reports and statistical data using native tools such as Microsoft® Excel®
- Generation of custom reports using third party applications
- Interfacing events data with applications and scripts built in-house.

To export events to CSV:

1. From **Events Browser > Views**, right-click a view and select **Export events**.



Screenshot 88: Export events tool

2. Specify or browse to the location where exported events are saved. Click **OK**.

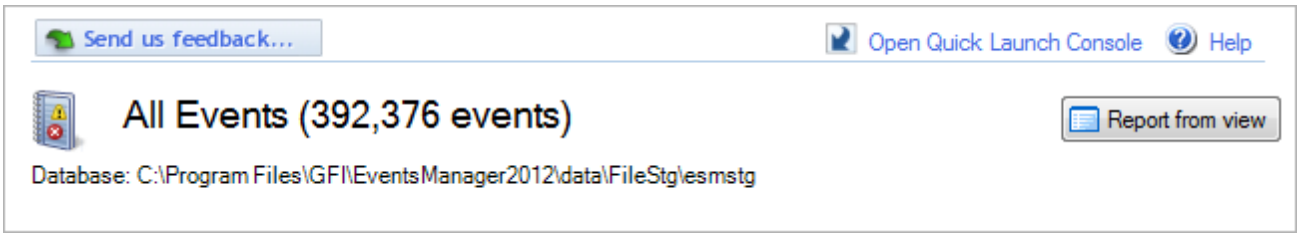
6.2.2 Creating reports from views

GFI EventsManager enables you to build your own custom reports (with graphs and statistics) based on a selected View from Events Browser.

> **Note**
>
> GFI EventsManager ships a selection of predefined reports. We recommend that you check the available reports prior to creating new ones to avoid having duplicate reports.

To generate a report from a view:

1. From **Events Browser > Views**, select a view.



Screenshot 89: Report from view button

2. From the top-right corner of the Events Browser, click **Report from view**.
3. From the **Create Report** dialog, configure the options from the tabs described below:

Table 40: Event Browser: Create new report

Tab	Description
General	Specify the new report name and add conditions.
Layout	Select the columns that you want to be visible in the report. You can also customize the order of appearance.
Chart	Select **Use graphical charts** to generate a report showing information in a chart. The available chart types are: » Pie chart » Bar chart » Line graph.
Schedule	Select **Use schedule** to enable report scheduling. Configure the generation date and frequency for the new report.

Note

For more information refer to Creating custom reports.

6.2.3 Deleting events

When collecting and processing event logs from a significantly large number of event sources, a number of unwanted logs are collected. To help you remove such event logs, GFI EventsManager includes a delete option. When events are deleted, they are:

- Removed from events browser
- No longer included in export/import jobs
- No longer included in reports.

After deleting an event, every other event of the same type, category and containing view are deleted as well.

Important

Before you delete event logs, ensure that you are abiding by legal compliance regulations. Deleting event logs may lead to legal penalties.

To delete events:

1. From **Events Browser** tab > **Views**, select a view.
2. Select an event that you want to delete. From **Actions**, click **Mark events as deleted**.
3. Click **Yes** to confirm delete or click **No** to cancel.

Viewing deleted events

Deleted event logs are stored in a separate database and can be viewed from the Events Browser.

To view deleted event logs:

1. Click **Events Browser** tab.
2. From the top-right pane, click **View deleted events**. The Events Browser automatically switches the database.

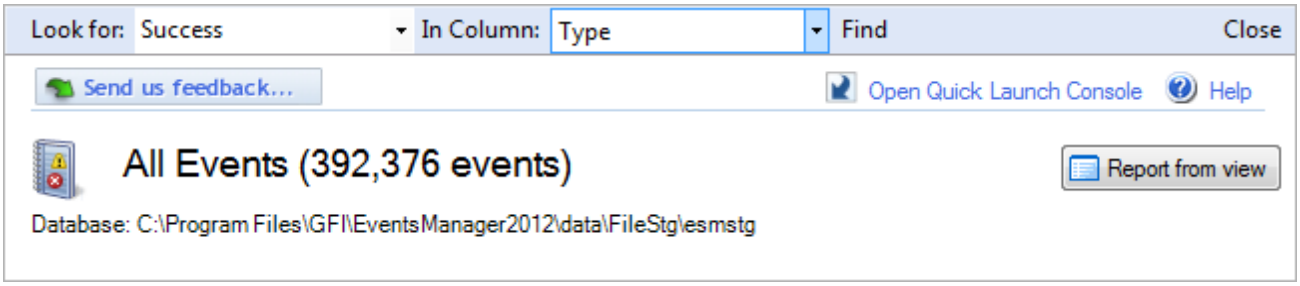
Note

To completely remove event logs from GFI EventsManager, you must run a **Commit Deletion** job on the selected database. For more information refer to Commit deletions.

6.2.4 Searching stored events

Use the event finder tool to search and locate specific events using simple customizable filters. To search for a particular event:

1. Click **Events Browser > Actions > Find events**.



Screenshot 90: Event finder tool

2. Configure the event search parameters through the options provided on top of the right pane. To trigger a case sensitive search, click **Options** and select **Match whole word**.

3. Click **Find** to start searching.

6.2.5 Identifying rules using the rule finder tool

GFI EventsManager enables you to identify the event processing rule which triggered the selected event log.

To identify the rule(s) used for a specific event:

1. From **Events Browser**, right-click an event log.

2. Click **Find Rule**. Doing so will take you to **Configuration** tab > **Event Processing Rules**. For more information refer to Events Processing Rules.

6.3 Managing Events Browser views

Event logs are automatically categorized in different folders, according to the event log type and the source from which it was generated. In GFI EventsManager, these folders are referred to as Views.

GFI EventsManager includes a comprehensive list of views that enable you to start categorizing processed event logs upon installation. New views can be created and the existing ones can be modified. The following sections provide with information about managing the Events Browser views:

- Creating Root Views and Views
- Editing a view
- Deleting a view

6.3.1 Creating Root Views and Views

In Events Browser, GFI EventsManager enables you to create the two different types of views described below:

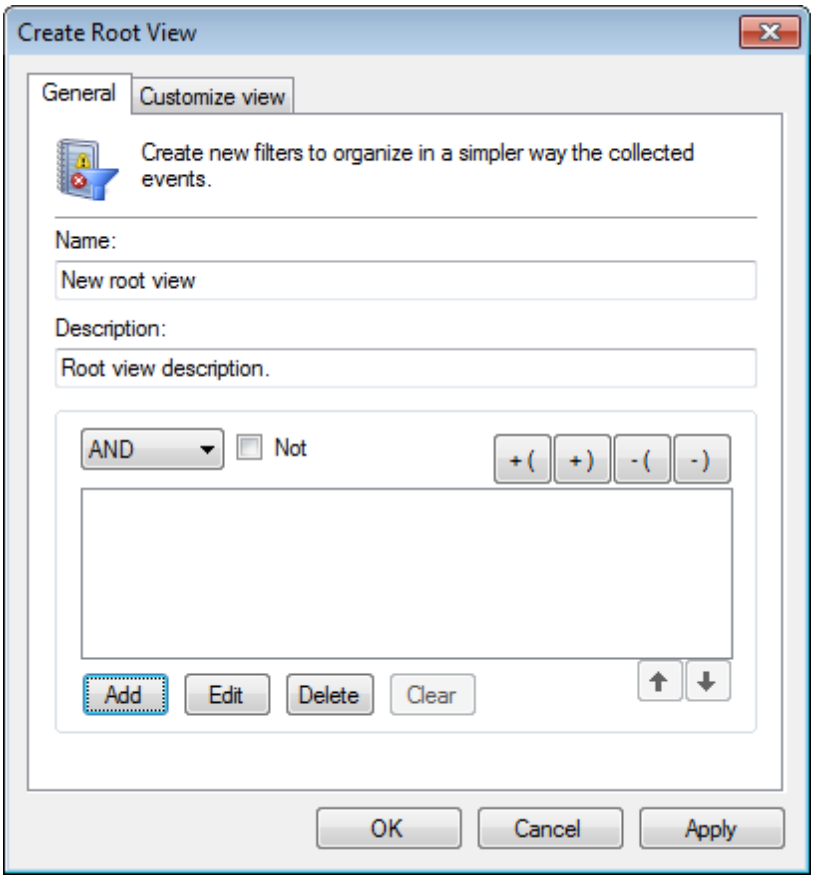
Table 41: Event Browser: Create new view

View	Description
Create root view…	Enables you to create top-level views which may contain a number of sub-views. This creates a new set of views beneath the ones that ship with the product (Example: **All Events** view).
Create view…	Create views within root views. Custom views can be added to the default root views and views.

To create a Root view/View:

1. From **Events Browser > Actions**, click **Create root view…/Create view…**

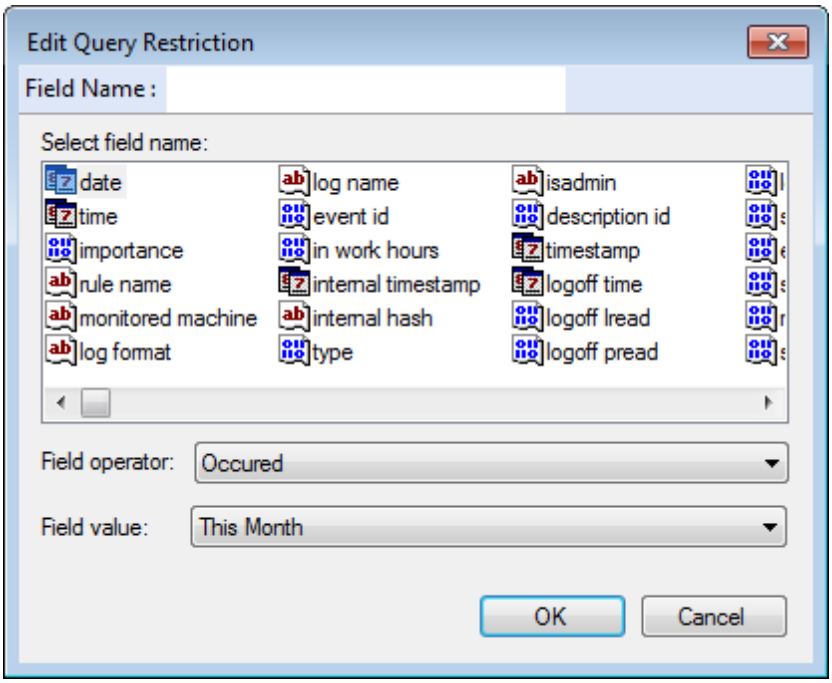
> **Note**
>
> Both options launch the same **Create view** dialog and are both configured in the same way. The difference is the positioning of the new custom view.



Screenshot 91: Custom view builder

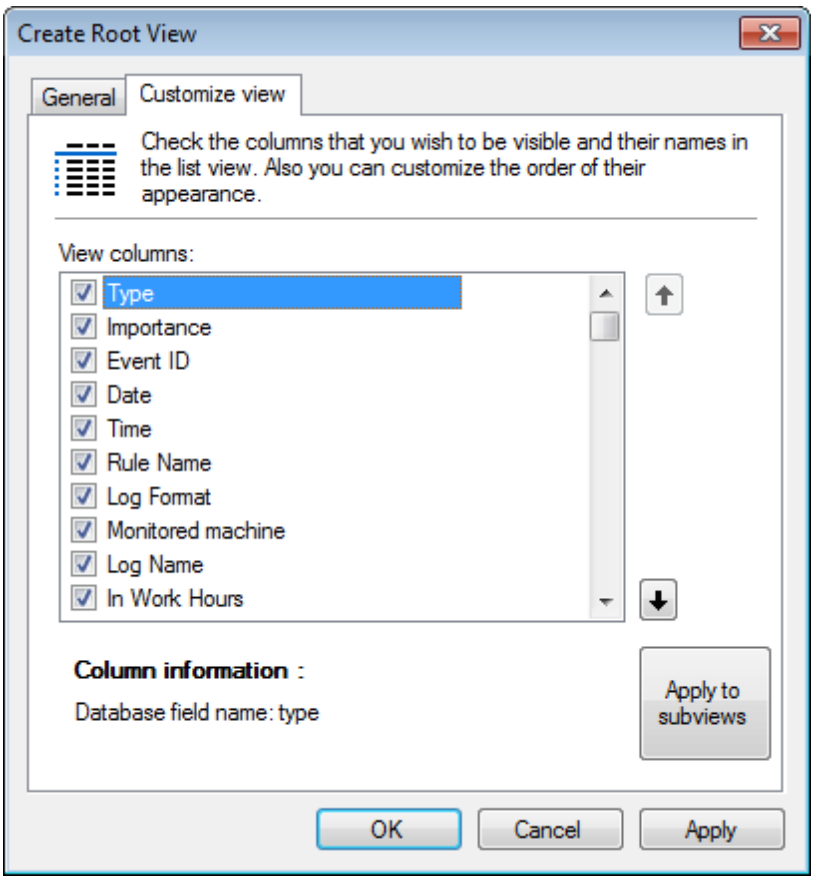
2. Key in a name and description for the new view.

3. Click **Add** to add filtering conditions to your view. If no conditions are specified, the view will display information from every event that is generated.



Screenshot 92: Edit view restriction

4. Select a field from the list of available fields and specify the **Field operator** and **Field value**. Repeat this step until all required conditions are specified. Click **OK**. For more information, refer to Defining Restrictions.

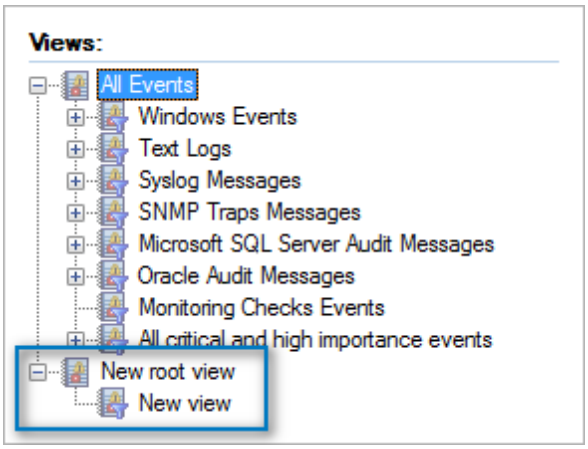


Screenshot 93: Customize View tab

4. Click **Customize view** tab to select the columns to show in the new custom view. You can also arrange their order of appearance using the **Up** and **Down** arrow buttons.

5. (Optional) Click **Apply to subviews** to apply the selected columns to all subviews of the root view.

6. Click **Apply** and **OK**.



Screenshot 94: Sample: New Root Views and Views

6.3.2 Editing a view

1. From **Events Browser > Views**, select the view to edit.

2. From **Actions** click **Edit view…**

3. From the View Properties dialog, add, edit or delete conditions according to your requirements.

6.3.3 Deleting a view

1. From **Events Browser > Views**, select the view to delete.

2. From **Actions**, click **Delete view**. Alternatively, right-click on the view you want to delete and select **Delete view**.

6.4 Customizing Events Browser layout

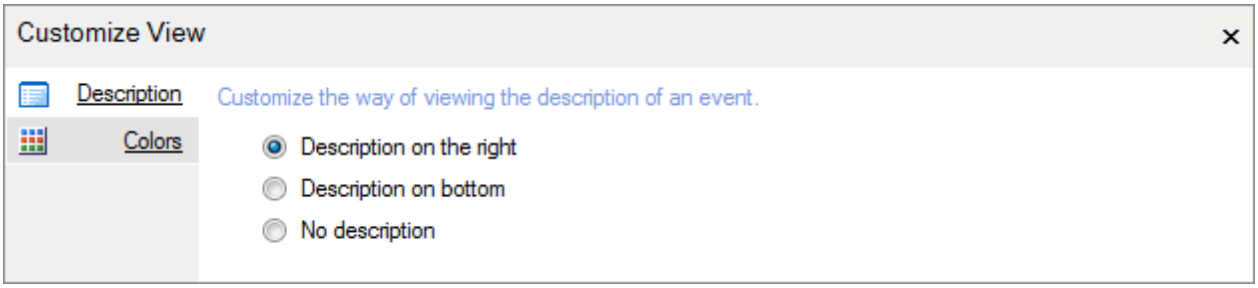
GFI EventsManager enables you to customize the Events Browser according to your preferences. You can reposition the description pane as well as modify event log color-coding options, used to facilitate identification of important events. The following sections provide you with information about customizing the Events Browser:

- Customizing description position
- Event color-coding options

6.4.1 Customizing description position

To change the position of the event description pane:

1. From **Events Browser > Common Tasks**, click **Customize browser layout > Description**.



Screenshot 95: Customize browser description

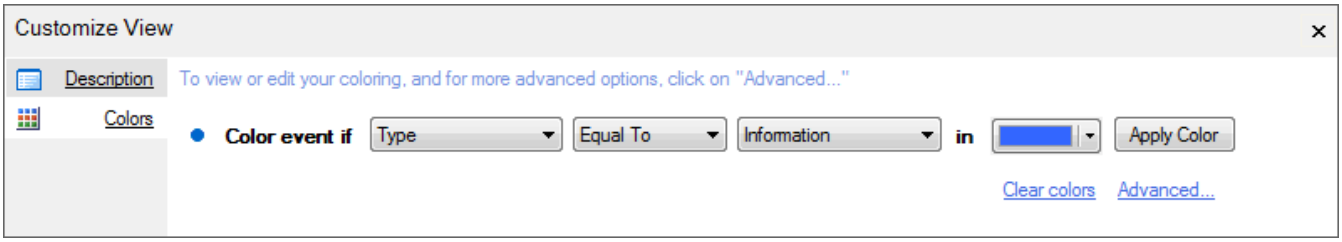
2. Select one of the options described below:

Table 42: Description pane positions

Option	Description
Description on the right	Places the description pane to the right of the events list.
Description on bottom	Places the description pane at the bottom of the events list.
No description	Removes description pane.

6.4.2 Event color-coding options

Use the event color-coding tool to tint key events in a particular color. This way the required events are easier to locate during event browsing.



Screenshot 96: Color coding configuration

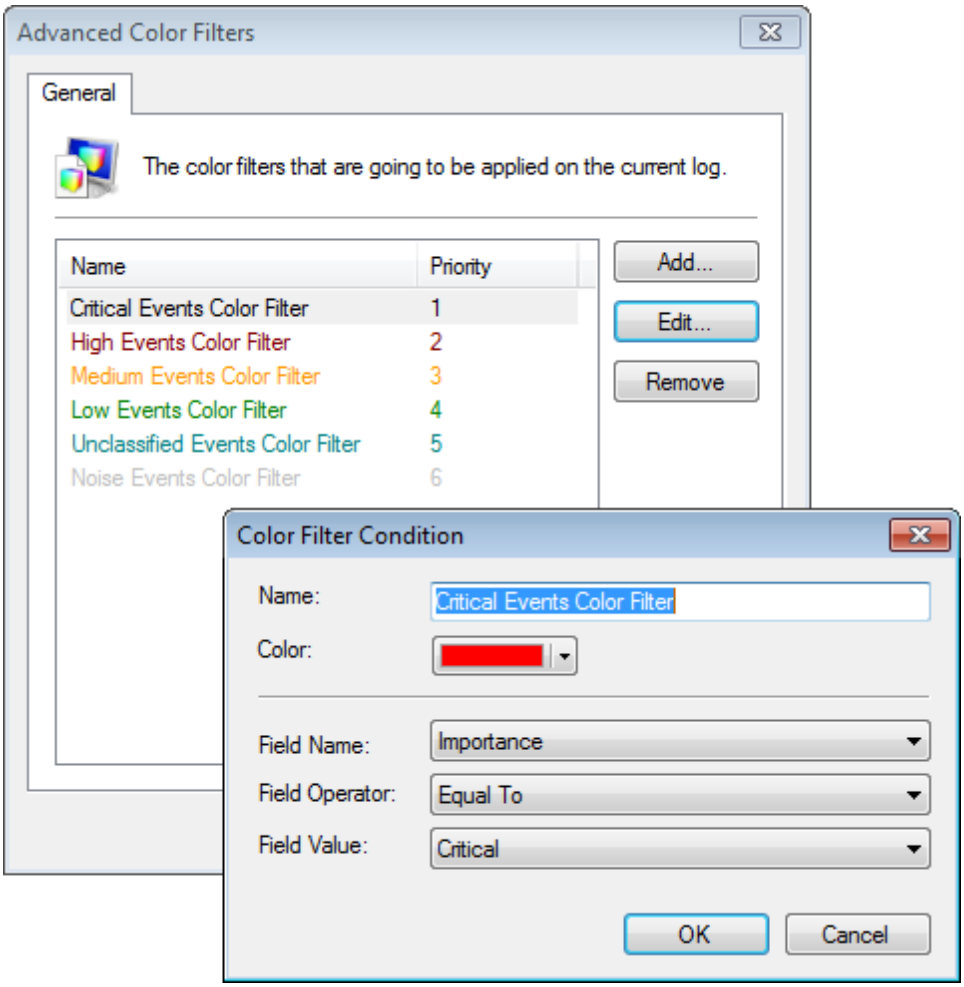
To assign a color code to a specific event:

1. From **Events Browser > Common Tasks** select **Customize browser layout > Colors**.
2. Specify event filtering parameters including the color to be applied to the sifted events.
3. Click **Apply Color**.

> **Note**
>
> Use the **Clear color** option to clear all color settings.

To assign different color-codes to multiple events:

1. From **Events Browser > Common Tasks** select **Customize view > Colors > Advanced…**



Screenshot 97: Advanced Color Filter

2. Click **Add** button. Specify filter name and configure event filter parameters.

3. Click **OK**.

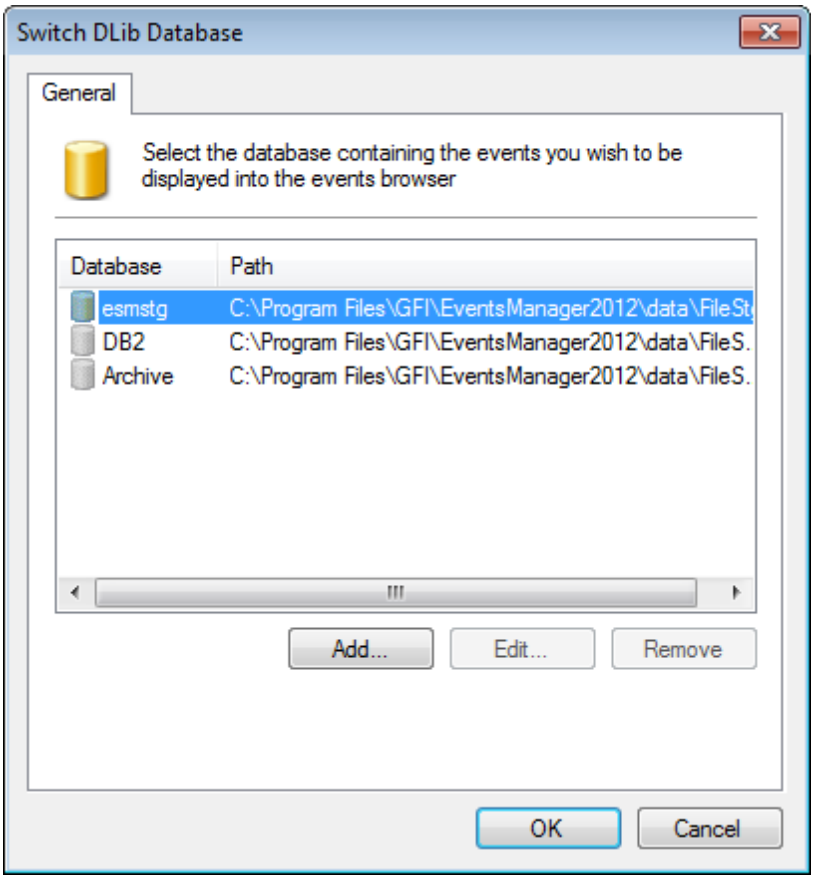
4. Repeat until all required event filter conditions have been configured. Click **OK**.

6.5 Browsing events from different databases

GFI EventsManager enables you to switch between different databases. Use this feature to browse events that have been exported or archived for further analysis or stored in different databases.

To switch databases:

1. Click **Events Browser > Common Tasks > Switch database**.



Screenshot 98: Switch database dialog

2. Select the database from the list of databases and click **OK**.

Note

You can click **Add…** to specify a path and a unique name to create a new database. Click **Edit…** to edit the specified information.

7 Activity Monitoring

This chapter provides you with information about monitoring the events collection processes. The **Status** tab is a dashboard that shows the status of GFI EventsManager as well as statistical information related to the events collected, processed and archived. The status monitor consists of three different dashboard views: **General** view, **Job Activity** view and **Statistics** view.

Topics in this chapter:

7.1 General Status view 134

7.2 Job Activity view 138

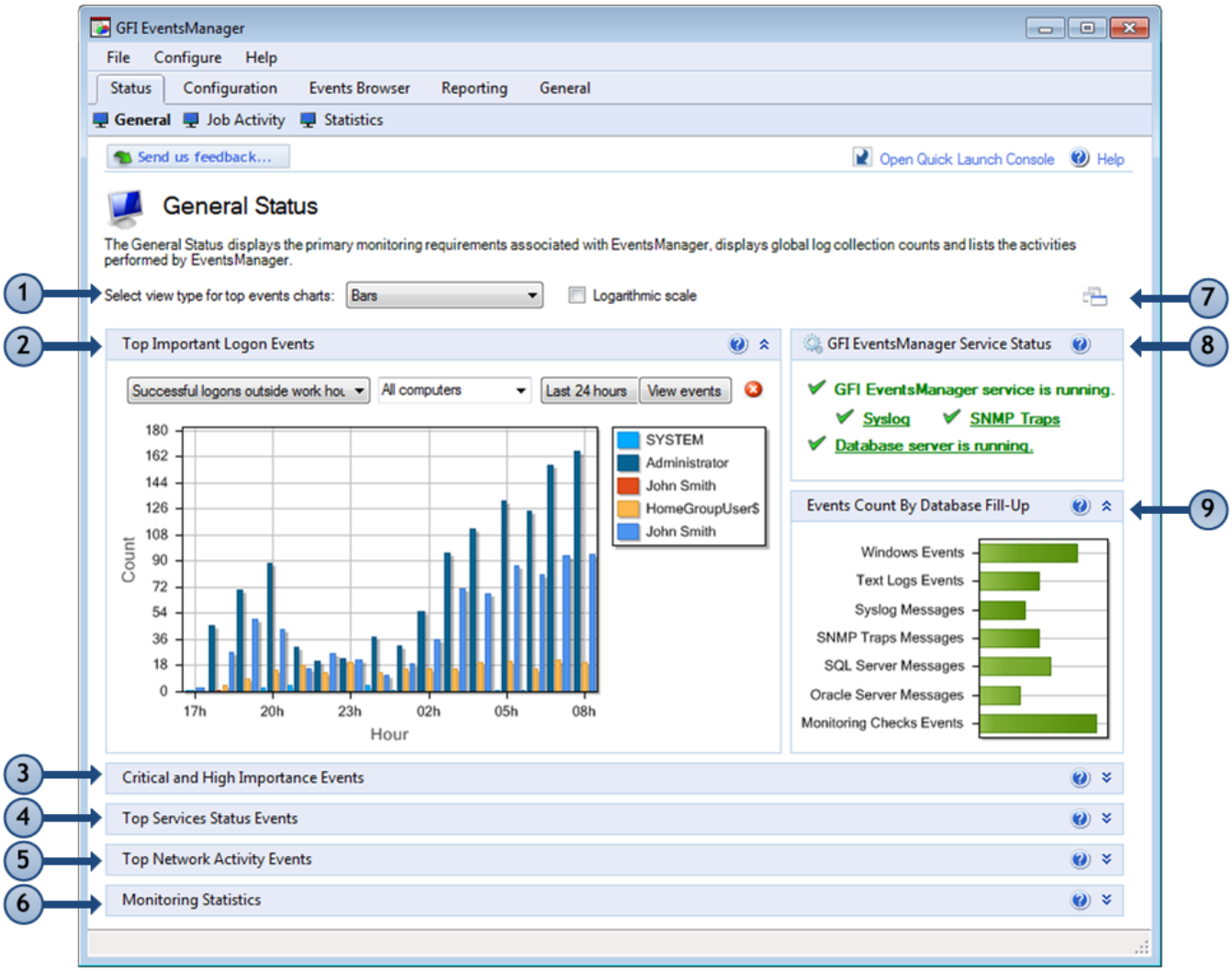
7.3 Statistics view 139

7.1 General Status view

This General Status view is used to:

- View the status of the GFI EventsManager event processing engine
- Access statistical information such as the number of logon events, critical events and service status events.

To access the **General** view, go to **Status** tab > **General**.



Screenshot 99: GFI EventsManager Status: General view

The General view consists of the sections described below:

Table 43: Status monitoring: General view sections

Section	Description
1	Use this section to select the chart type for top events.
2	The **Top Important Log Events** section provides statistical information about: » Top 10 successful Logon events outside working hours » Top 10 important Logon events during working hours » Top 10 failed Logon events. Events in this section are filtered by: » **Machine**: Select a machine or key in a machine name in the drop down list » **Period**: The time period when the events occurred (Last hour, Last 24 hours, Last 7 days or a specific date).

Section	Description
3	The **Critical and High Importance Events** section provides statistical/graphical information about critical events collected from all event sources. This graph shows the event processing rules that collected and processed the events for a particular period. From the drop down lists, select the type of information to display. Select from: » **Grouping**: Determines how events are grouped; such as Events, Computers, Computer groups, Events/Computers or Events/Computer groups » **Event type**: Select the type of data to display (Windows®, Text Logs, Syslog, SNMP, Active Monitoring Logs, SQL and Oracle audit) » **Alert type**: Specify the alert severity; such as All alerts, Critical or High » **Period**: Specify the time period when the events occurred (Last hour, Last 24 hours, Last 7 days or a specific date). **NOTE** This section also displays the vulnerability results monitored by GFI LanGuard. **NOTE** For detailed information about the different types of important events shown in this view, download the Microsoft® Security Monitoring and Attack Detection Planning Guide from http://go.gfi.com/?pageid=esm_smad_plan.
4	The **Top Service Status Events** displays the top 10 services that caused the selected event. A service can generate events when: » Terminated with an error » Failed to load » Failed to start » Timed out » Stopped » Started. The graph shows the frequency of these events sorted by service type and/or by computer generating the event. Select a machine or service from the drop down lists or key in the required criteria to customize the graph results. **Note** To collect services information, event sources must have Audit system events policy enabled. For more information, refer to Enabling event source permissions manually (page 326).

Section	Description
5	The **Top Network Activity Events** section displays details of the top 10 network activities (inbound and outbound). Network activity consists of all type of traffic that is generated by various protocols including SMTP, HTTP, FTP and MSN traffic. The network activities displayed can be filtered by: » Applications » Source Addresses » Destination Addresses » Computers » Ports » Users. Select parameters from the drop down lists or key in the values to filter the type of chart displayed. **Note** The network activity shown in the chart applies only to computers running Microsoft® Windows® Vista or later. **Note** To collect network activities, event sources must have Object auditing and Process tracking enabled. For more information refer to Enabling event source permissions manually.
6	The **Monitoring Statistics** section displays status information about active Active Monitoring you are running on event sources. The information displayed in this section is refreshed every 20 seconds and you provides the: » Check name » Success/Fail count » Number of generated events » Check date and time » Check type. Select a row and click **View Events** to view the pertaining logs that were generated when the check failed/succeeded.
7	Click the **Arrange Window** icon to automatically fit all graphs in the management console.
8	The GFI EventsManager **Service Status** is used to view: » The operational status of GFI EventsManager service/event processing engine » The operational status of the Syslog server » The operational status of the SNMP Traps server » The operational status of the database server currently in use by GFI EventsManager. **Note** Click the service name to edit the service settings. **Note** Click **Database server is running** to switch between different databases. For more information refer to Switching between file storage databases.

Section	Description
9	The **Events Count By Database Fill-Up** displays: » The horizontal bars represent the number of events stored in the database backend, sorted by event log type » The date and time of the last backup » The date and time of the next scheduled backup. The bar color turns from green to red as the database is populated with events.

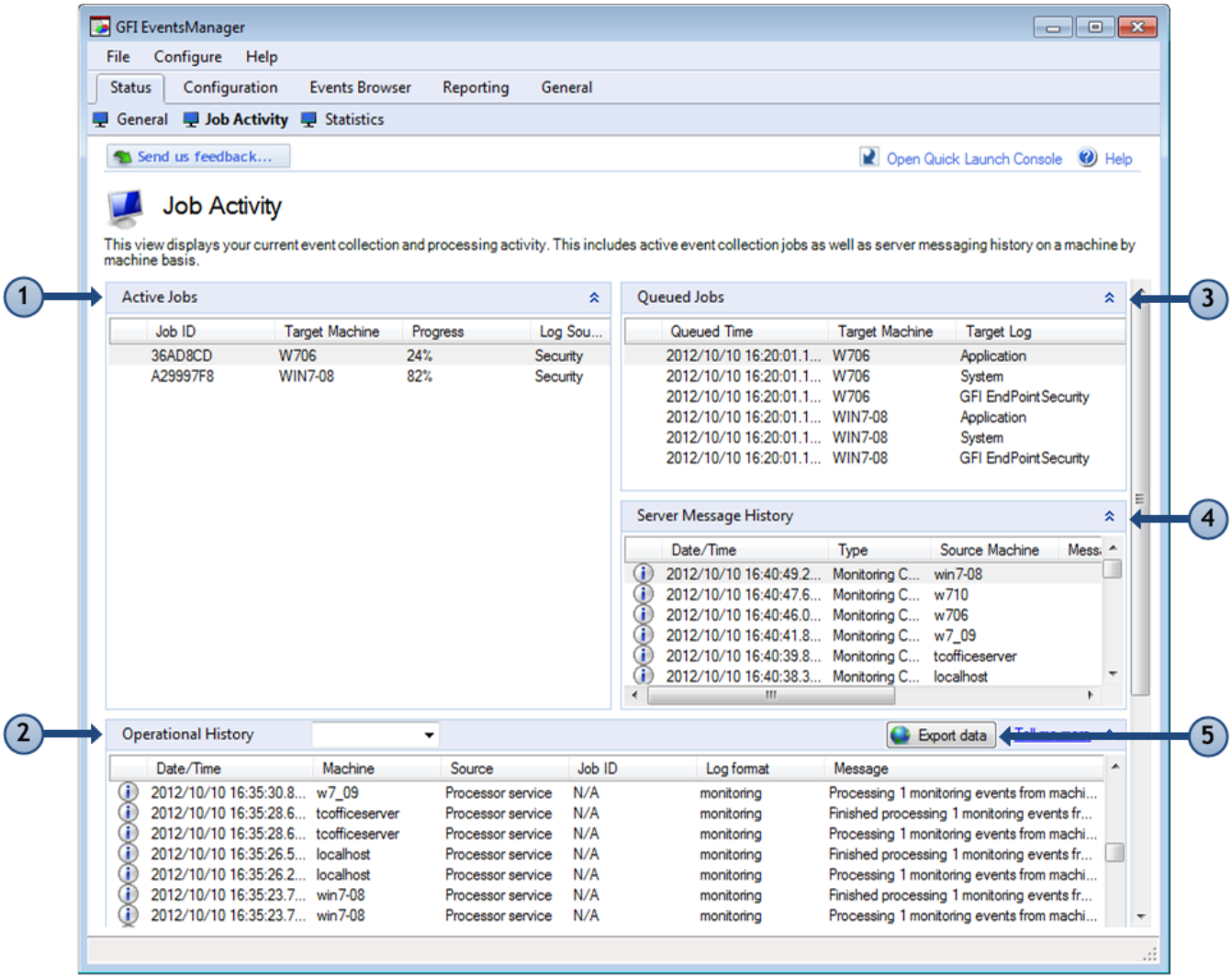
Note

Double-click the graph to open the graph in a new window. When a 3D graph is selected, the new window allows you to rotate, zoom or resize the graph. Use the **Export to image** button to export the graph.

7.2 Job Activity view

This view displays your current event collection and processing activity. This includes active event collection jobs as well as server messaging history on a machine by machine basis.

To access the **Job Activity** view, go to **Status** tab **> Job Activity**.



Screenshot 100: GFI EventsManager Status: Job Activity view

The information provided in this view is divided into the following dedicated sections:

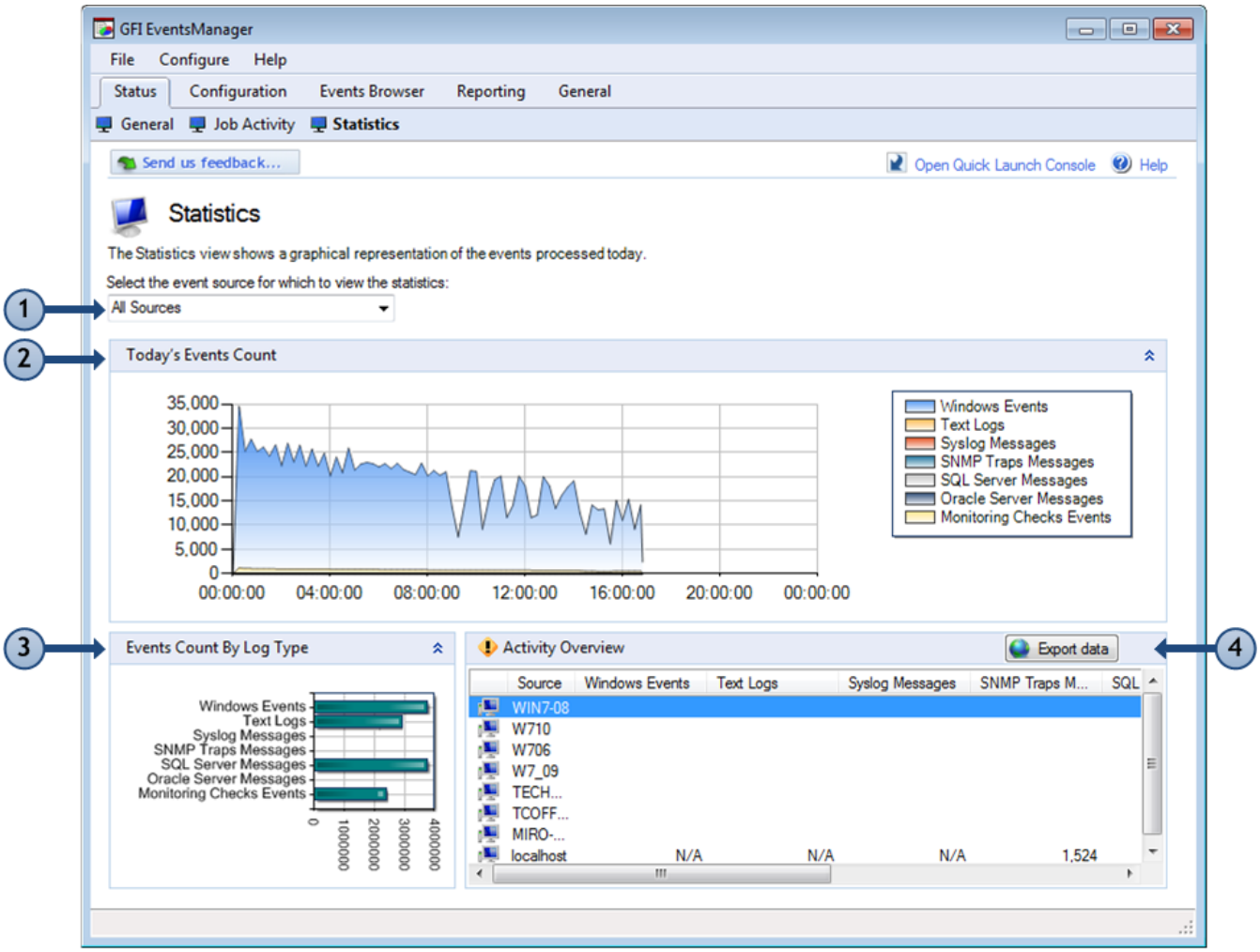
Table 44: Status monitoring: Job activity view

Section	Description
1	The **Active Jobs** section provides a list of all event collection jobs currently taking place on every event source/machine. The information provided includes the job progress as well as the Log Source from which events are being collected.
2	The **Operational History** section shows an audit trail of the event collection operations performed by GFI EventsManager. The information provided includes errors and information messages generated during the event collection process as well as the name of the log file that was being processed on the event source. **NOTE** Operational history logs can be exported using the Export data button. For more information refer to Generating reports.
3	The **Queued Jobs** section provides a list of all pending event collection jobs on a machine by machine basis. The information provided includes the event source from which events will be collected as well as the queuing time and type of log to collect.
4	The **Server Message History** section displays a list of all server messages (SNMP Traps and Syslog) that were received by GFI EventsManager. The information provided includes the total number of messages sent by every event source, message count and the date/time when the last message was received.
5	Click **Export data** to generate Operational History reports.

7.3 Statistics view

The **Statistics** view is used to display the daily event activity trends and statistics of a particular computer or entire network.

To access the **Statistics** view, go to **Status** tab > **Statistics**.



Screenshot 101: GFI EventsManager Status: Statistics view

The information provided in this view is divided into the following dedicated sections:

Table 45: Status monitoring: Statistics view

Section	Description
1	Use this drop-down menu to select what information is displayed. Select between **All sources** or select specific sources to view their information accordingly.
2	The **Today's Events Count** graphically represents the daily event collection trend on a machine by machine basis as well as on a network by network basis. A color scheme is used to differentiate between Windows®, Text Logs, Active Monitoring Logs, Syslog and SNMP Traps events.
3	The **Events Count By Log Type** represents the number of Windows®, Text Logs, Syslog and SNMP Traps events collected by GFI EventsManager from a particular machine or network.
4	The **Activity Overview** section provides information about: » The total number of Windows®, Text Logs, Active Monitoring Logs, Syslog and SNMP Traps events processed on a machine by machine basis » The date/time of the last event collection performed from every machine. Click **Export data** to generate Activity Overview reports.

8 Reporting

This chapter provides information about the fully-fledged reporting engine of GFI EventsManager. It ships with a number of reports including technical and executive level reports showing graphical and statistical information based on hardware and software managed by GFI EventsManager.

Topics in this chapter:

8.1 Navigating the Reports tab 142

8.2 Available reports 143

8.3 Managing reports 144

8.4 Creating a root report 146

8.5 Creating custom reports 151

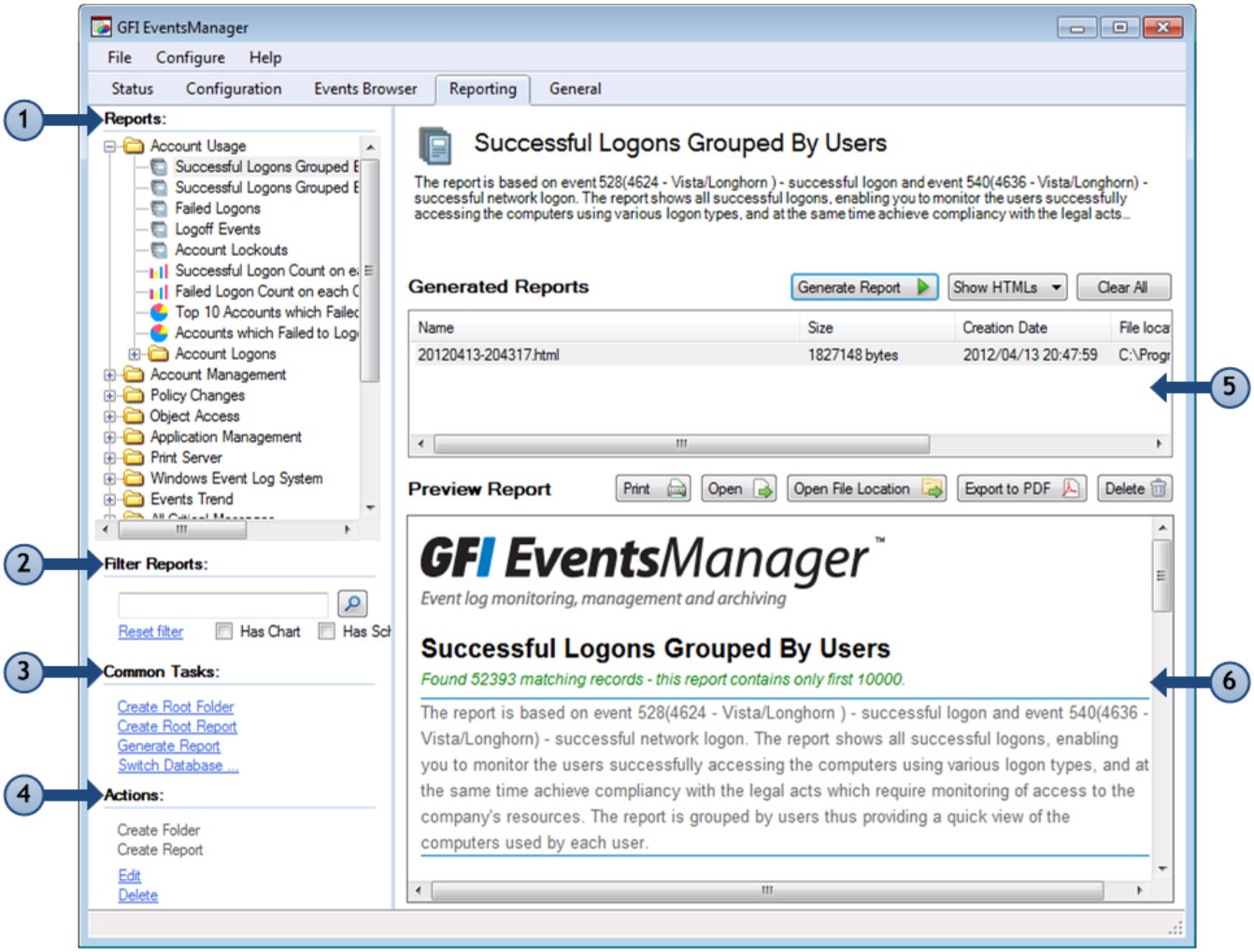
8.6 Generating reports 158

8.7 Analyzing reports 168

8.8 Defining column headings 169

8.9 Customizing HTML reports 170

8.1 Navigating the Reports tab


GFI EventsManager
File
Configure
Help
Status
Configuration
Events Browser
Reporting
General
1
Reports:
Account Usage
Successful Logons Grouped E
Successful Logons Grouped E
Failed Logons
Logoff Events
Account Lockouts
Successful Logon Count on e
Failed Logon Count on each C
Top 10 Accounts which Failed
Accounts which Failed to Log
Account Logons
Account Management
Policy Changes
Object Access
Application Management
Print Server
Windows Event Log System
Events Trend
2
Filter Reports:
Reset filter
Has Chart
Has Sch
3
Common Tasks:
Create Root Folder
Create Root Report
Generate Report
Switch Database ...
4
Actions:
Create Folder
Create Report
Edit
Delete
Successful Logons Grouped By Users
The report is based on event 528(4624 - Vista/Longhorn) - successful logon and event 540(4636 - Vista/Longhorn) - successful network logon. The report shows all successful logons, enabling you to monitor the users successfully accessing the computers using various logon types, and at the same time achieve compliancy with the legal acts...
Generated Reports
Generate Report
Show HTMLs
Clear All
Name
Size
Creation Date
File loca
20120413-204317.html
1827148 bytes
2012/04/13 20:47:59
C:\Progr
5
Preview Report
Print
Open
Open File Location
Export to PDF
Delete
GFI EventsManager
Event log monitoring, management and archiving
Successful Logons Grouped By Users
Found 52393 matching records - this report contains only first 10000.
The report is based on event 528(4624 - Vista/Longhorn) - successful logon and event 540(4636 - Vista/Longhorn) - successful network logon. The report shows all successful logons, enabling you to monitor the users successfully accessing the computers using various logon types, and at the same time achieve compliancy with the legal acts which require monitoring of access to the company's resources. The report is grouped by users thus providing a quick view of the computers used by each user.
6

Screenshot 102: Navigating the Reporting UI

The Reporting tab consists of the sections described below:

Table 46: Navigating the Reporting tab

Section	Description
1	The **Reports** section contains all the predefined reports that ship with the product. Use this section to organize and generate various reports from technical to executive type.
2	Find reports rapidly, using the available filtering options. Through **Filter Reports** options, you are able to search for reports that contain charts and are generated based on a schedule.
3	The **Common Tasks** section enables you to quickly launch typical operations such as creating folder and report views to organize reports and generating reports.
4	From **Actions**, create, edit or delete reports according to your needs.
5	Use the **Generated Reports** section to view the history of a selected report (from Section 1). This enables you to regenerate and export the report to HTML and/or PDF.
6	The **Preview Report** section provides a view of a selected, generated report. Use the control buttons to Print, Open, Export or Delete reports directly from this section.

8.2 Available reports

GFI EventsManager's extensive report list contains reports for various requirements designed to facilitate reporting as much as possible. The following report categories are included in GFI EventsManager by default. GFI EventsManager allows you to use the existing reports as templates to create your own ones. Each category in the table below contains a number of reports that can be used out of the box or customized to fit your requirements:

Table 47: Available reports

Category	Description
Account Usage	Use the reports in this category to identify user logon issues. The event details shown in these reports include successful/failed user logons and locked user accounts.
Account Management	Use the reports in this category to generate a graphical overview of important events that took place across your entire network. The event details shown in these reports include changes in user and computer accounts as well as changes in security group policies.
Policy Changes	Use the reports in this category to identify policy changes effected on your network.
Object Access	Use the reports in this category to identify object access issues. The event details shown in these reports include successful/failed object access and objects that have been deleted.
Application Management	Use the reports in this category to identify faulty applications and application installation and removal issues. The event details shown in these reports include applications that have been installed or removed as well as applications, which are crashing and hanging.
Print Server	Use the reports in this category to display details related to printing events. Details provided in these reports include documents that have been printed, the users that triggered the printing event and the date/time when the printing operation took place.
Windows Event Log System	Use the reports in this category to identify audit failures and important Windows® event log issues. Details provided in these reports include the starting and stopping of event log services, clear log operations as well as errors generated during event logging.
Events Trend	Use the reports in this category to display statistical information related to event generation. Charts provided enumerate the 10 computers and users with most events. Other reports provide event counts on a network-wide basis as well as on a computer-by-computer basis. Reports in this category can be generated for each main time - by hour, day, week or month.
All Critical	Use the reports in this category to display information related to critical Windows® events, Syslog, Text Logs, Custom Events, SNMP Traps and SQL Server® Audit events. The charts provided enumerate the 10 most critical events.
Miscellaneous, Customizable	Use the reports in this category to generate reports that offer broad customization. These can be used to generate reports based on any Windows® event log, using filtering conditions and grouping modes that are not covered by the other default reports.
PCI DSS Compliance / GCSx Code of Connection Requirements / SOX Compliance / HIPAA Compliance / GLBA Compliance	Use the reports in these categories to generate legal compliance regulations reports.
General and Security Requirements	Use the reports in this category to generate various reports required by several GCSx Code of Connection memos.
LOGbinder SP reports	Use the reports in this category to generate reports related to Microsoft® SharePoint® audit events.

8.3 Managing reports

Reports are organized in a tree structure enabling you to easily find and generate the required report. GFI EventsManager includes various options that allow you to easily maintain the reports structure as the number of reports increase by time.

This section contains information about:

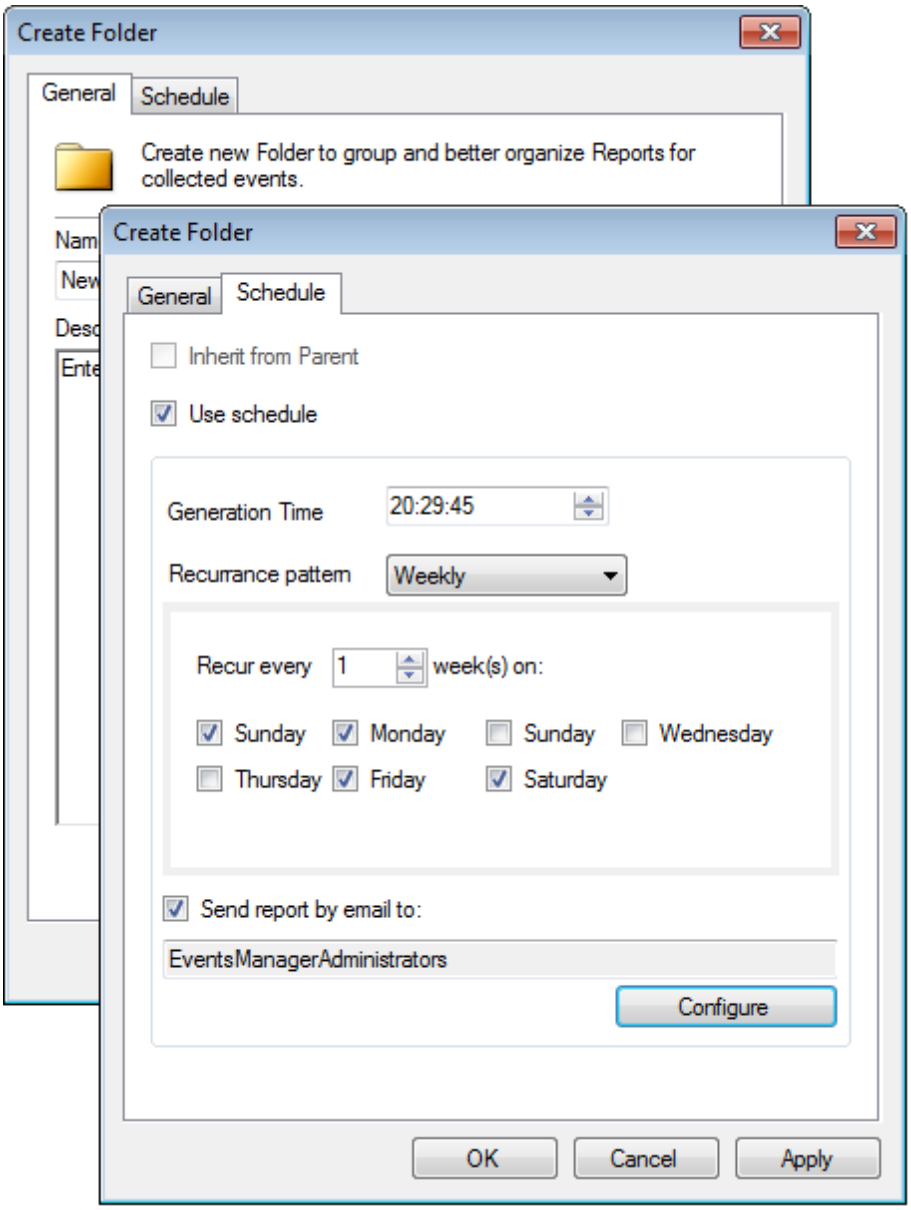
- Creating a root folder
- Creating a folder
- Creating a root report
- Creating custom reports
- Defining column headings

8.3.1 Creating a root folder

Root folders are top-level folders which may contain one or more sub-folders or reports.

To create a root folder:

1. From **Reporting** tab **> Common Tasks**, click **Create Root Folder**.



Screenshot 103: Create Report Folder dialog

2. From the **General** tab, specify a name and a description (optional) for the new folder.

3. Click **Schedule** tab and select **Use schedule** to configure a schedule for the reports included in this new folder. Configure the options described below:

Table 48: Create report folder: Schedule options

Option	Description
Inherit from Parent	Select when the new folder is part of a root folder that already has scheduling configured.
Use schedule	Select **Use Schedule** to enable scheduling of the reports contained in the new folder.
Generation time	Specify the time when reports are generated.
Recurrence pattern	Specify the report generation frequency. Select from **Daily**, **Weekly** or **Monthly** pattern and configure the respective parameters.
Send report by email to	Select this option to enable email notifications. Click Configure to select the users from the Select users and groups… dialog. **NOTE** Configure alerting options before using this feature.

4. Click **Apply** and **OK**.

8.3.2 Creating a folder

GFI EventsManager allows you to create as many recurring folders as required.

To create a folder:

1. From **Reporting** tab > **Reports**, right-click a root or sub-folder and select **Create Folder**.

2. From the **General** tab, specify the name and description (optional) for the new group.

3. Click **Schedule** tab and configure the required schedule settings.

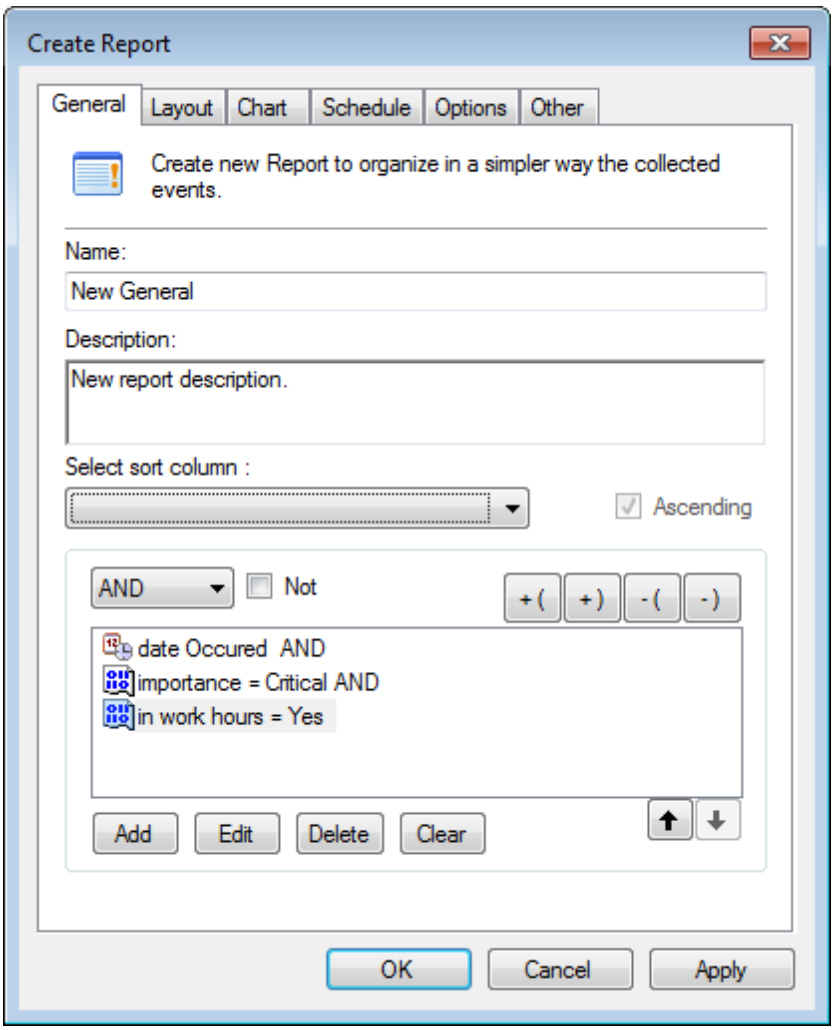
4. Click **Apply** and **OK**.

8.4 Creating a root report

Root reports behave in the same way as root folders. These are created at the top level and may contain a number of sub reports. For example, you can create a root report that generates on monthly basis, and contains information about successful logons, failed logons and account lockouts. It's sub-reports would only contain information about specific parts of the root report, such as failed logons only, generated on daily basis.

To create a root report:

1. From **Reporting** tab > **Common Tasks**, click **Create Root Report**.

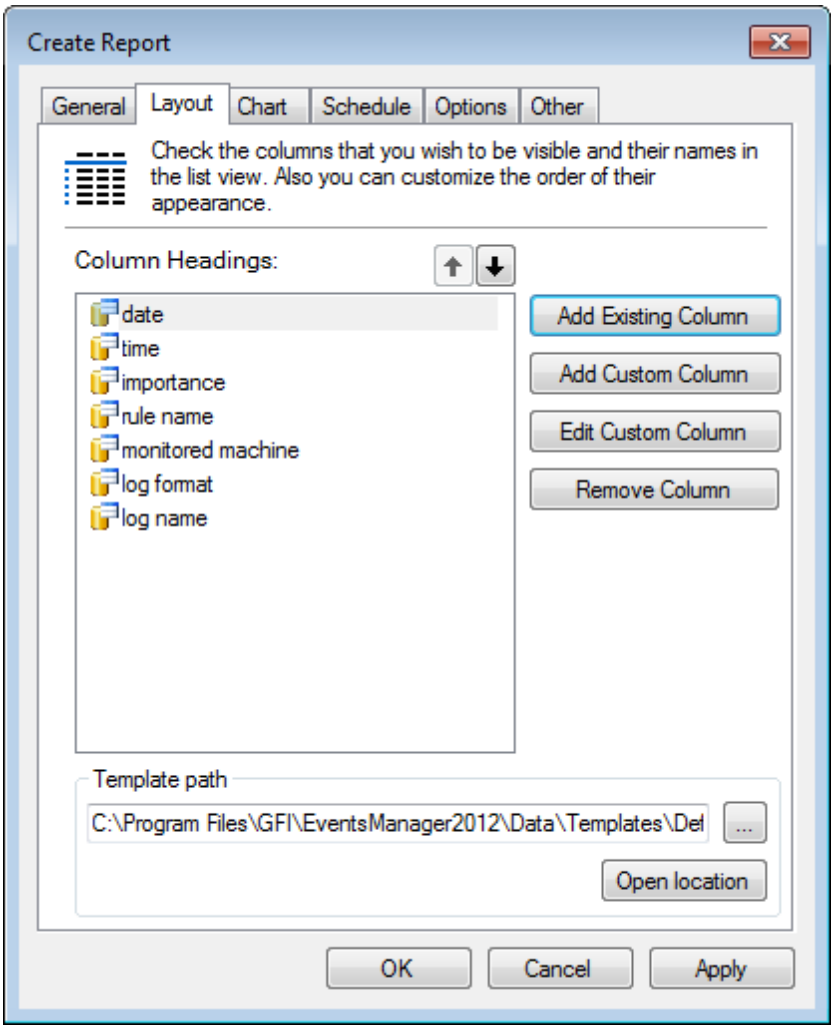


Screenshot 104: Creating a root report

2. From the **General** tab, specify a name and description (optional) for the new root report.

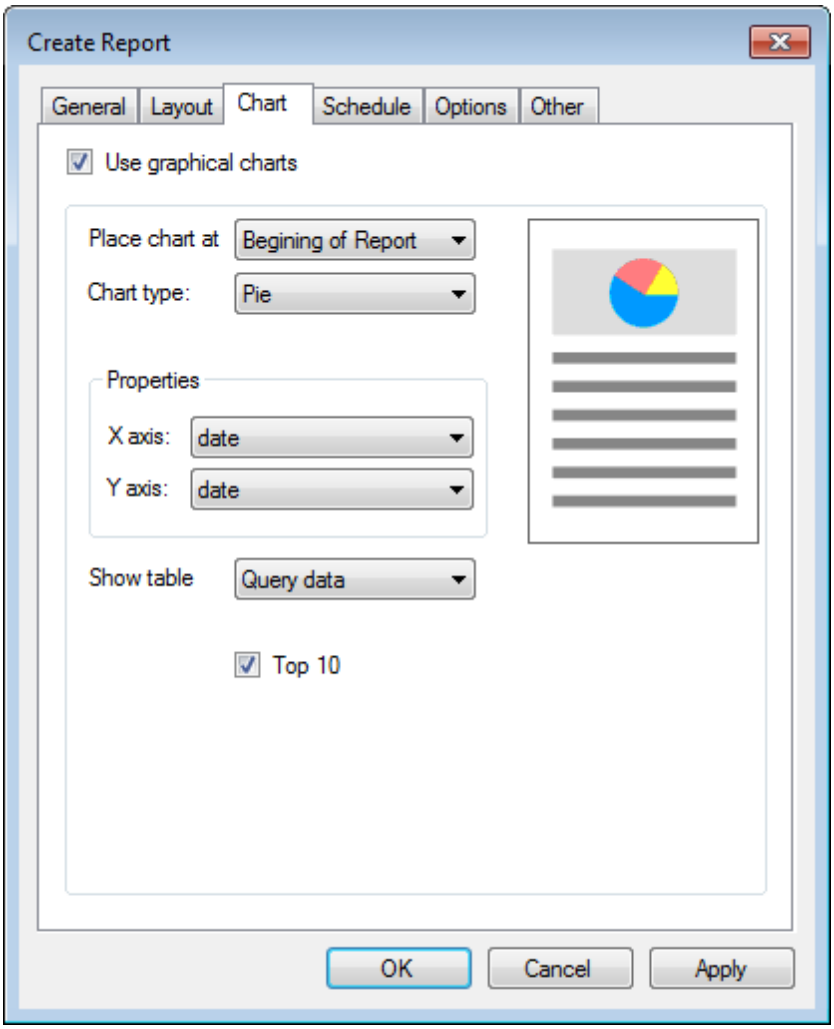
3. Click **Add** to select a field on which to base the query condition. For the selected field, specify the **Field Operator** and **Field Value**. Click **OK**.

> **Note**
>
> Repeat this step until all the required fields are selected. For more information refer to Building query restrictions.



Screenshot 105: Configuring new root report layout options

4. Click **Layout** tab and add the column headings that you want to be visible in the report. If you have a saved report template, click **Open location** to browse and load your template. For more information refer to Defining column headings.



Screenshot 106: Inserting a chart in a new root report

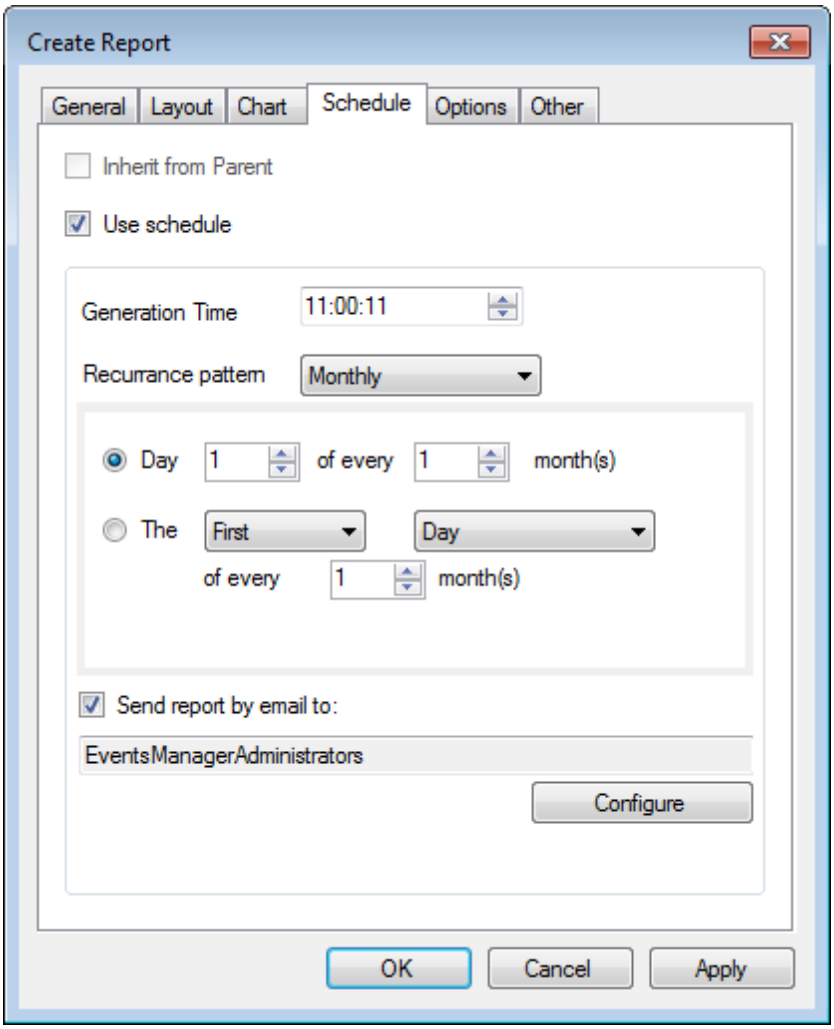
5. (Optional) Click **Chart** tab and select **Use graphical charts** to include graphs in your report.

6. From the **Place chart at** drop-down menu, specify the location of the chart. Select from:

- Beginning of Report
- End of Report.

7. From **Properties > X axis** and **Y axis**, configure the X and Y Axis properties. I.e. select the data represented in the chart.

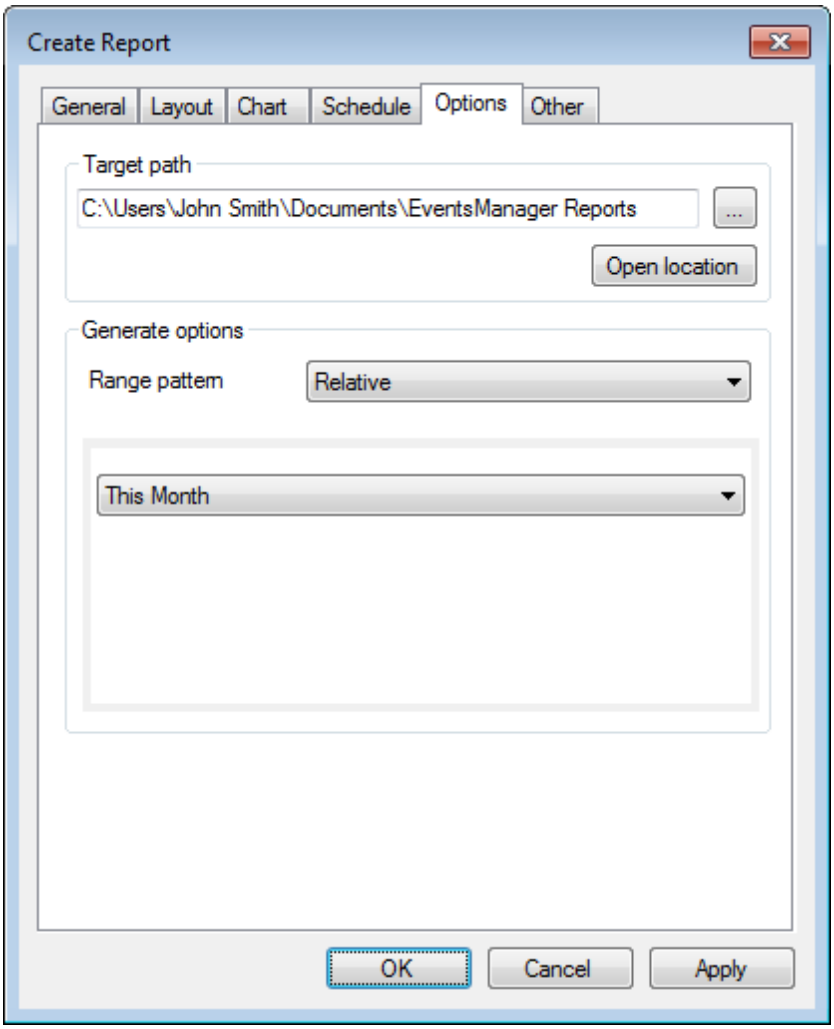
8. Select **Top 10** to view the Top 10 records only.



Screenshot 107: Configuring the schedule for when the report is generated

9. (Optional) Click **Schedule** tab and configure schedule settings.

10. Select **Send report by email to** and click **Configure** to select the recipients of this report.



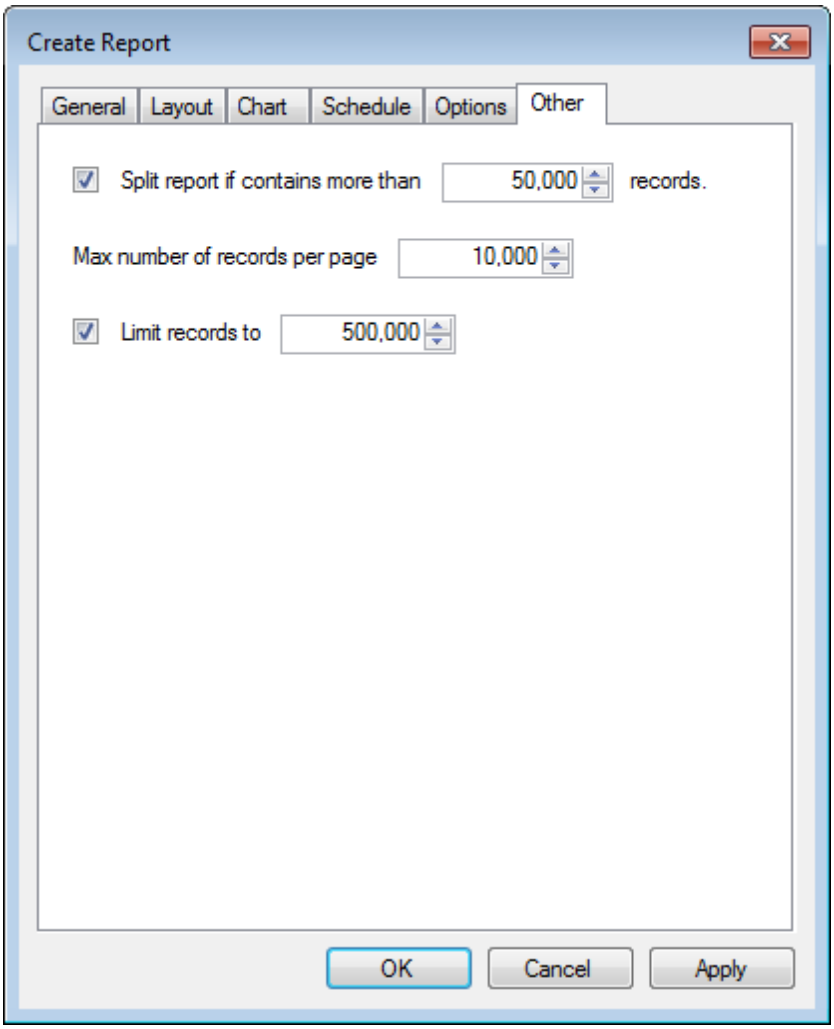
Screenshot 108: Create new report Options

11. Click **Options** tab and specify the path to where the report generates to in the **Target path** area.

12. From the **Range pattern** drop-down menu, select the options described in the table below:

Table 49: Range pattern options

Pattern	Description
All Time	Select **All Time** to generate the report based on information from all the related logs.
Relative	Generate the report based on events from: » Today » Yesterday » Last 7 Days » This Month » Last Month.
Day	Specify a single day that you want to base your report on.
Month	Specify a month and year that you want to base your report on.
Date Range	Specify a **From** and **To** date to base report information on events collected in the specified time period.



Screenshot 109: Record limit settings

13. Click **Other** tab to configure report record limits. Available options are described in the table below:

Table 50: Report record settings

Option	Description
Split report if it contains more than {X} records	Select the checkbox to enable record limit per report. GFI EventsManager automatically creates a new report for every number of records you specify. Example: if you key in 50, 000 and the report contains 150, 000 records, GFI EventsManager generates three reports.
Max number of records per page	Specify the number of records that are displayed in a single page.
Limit records to	Specify the maximum number of records that are included in the report. Records that exceed the limit are ignored.

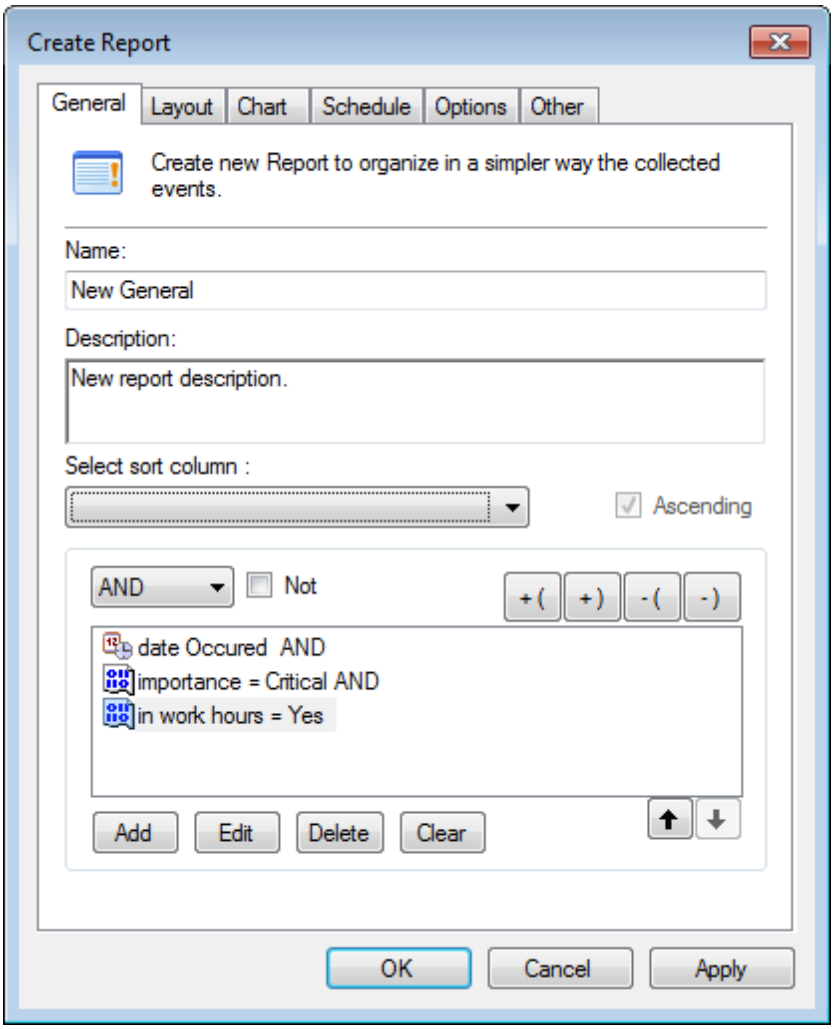
14. Click **Apply** and **OK**.

8.5 Creating custom reports

Creating custom reports requires planning while setting up conditions. Conditions are set to determine what is filtered and presented in the report. Failing to configure conditions properly generates unwanted noise and inaccurate information.

To create a new custom report:

1. From **Reporting** tab > **Reports**, right-click a root folder/folder/root report and select **Create Report**.

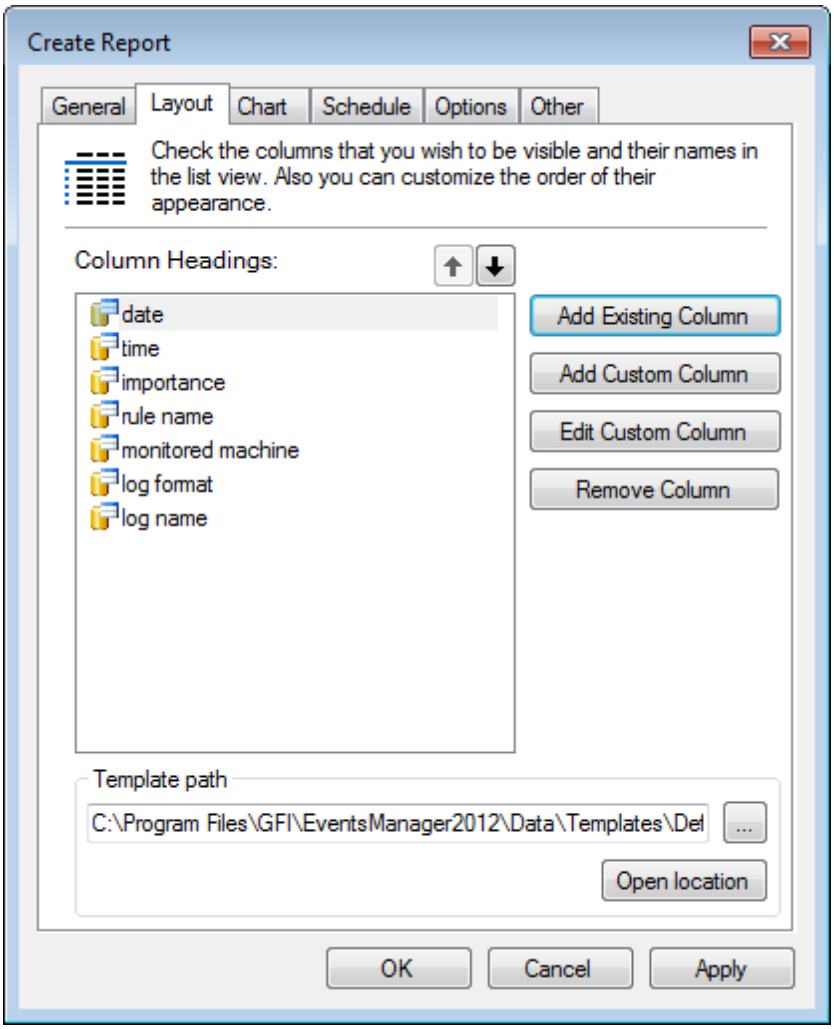


Screenshot 110: Creating a root report

2. From the **General** tab, specify a name and description (optional) for the new root report.

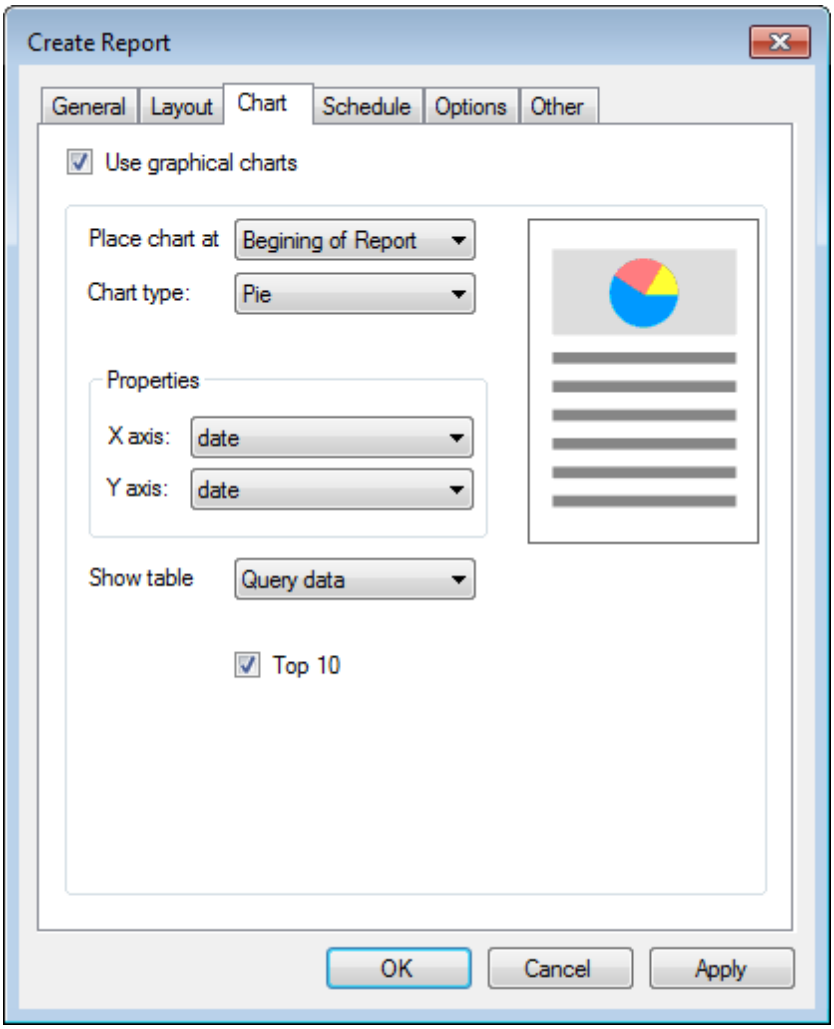
3. Click **Add** to select a field on which to base the query condition. For the selected field, specify the **Field Operator** and **Field Value**. Click **OK**.

> **Note**
>
> Repeat this step until all the required fields are selected. For more information refer to Building query restrictions.



Screenshot 111: Configuring new root report layout options

4. Click **Layout** tab and add the column headings that you want to be visible in the report. If you have a saved report template, click **Open location** to browse and load your template. For more information refer to Defining column headings.



Screenshot 112: Inserting a chart in a new root report

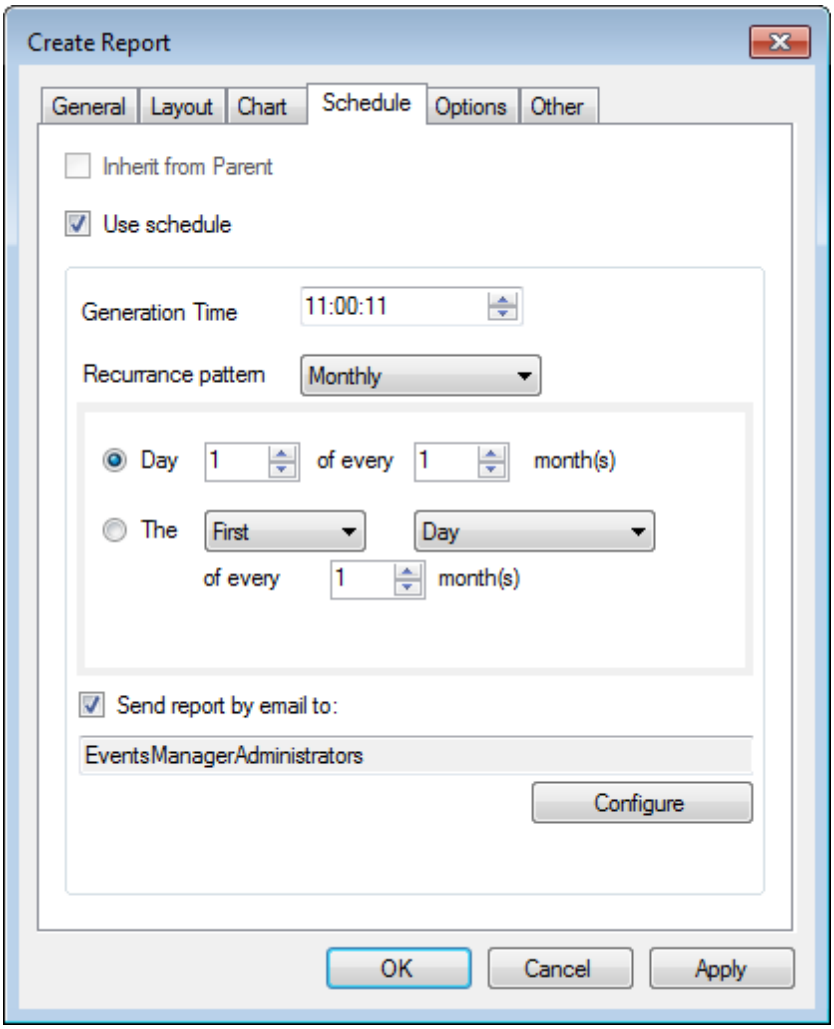
5. (Optional) Click **Chart** tab and select **Use graphical charts** to include graphs in your report.

6. From the **Place chart at** drop-down menu, specify the location of the chart. Select from:

- Beginning of Report
- End of Report.

7. From **Properties > X axis** and **Y axis**, configure the X and Y Axis properties. I.e. select the data represented in the chart.

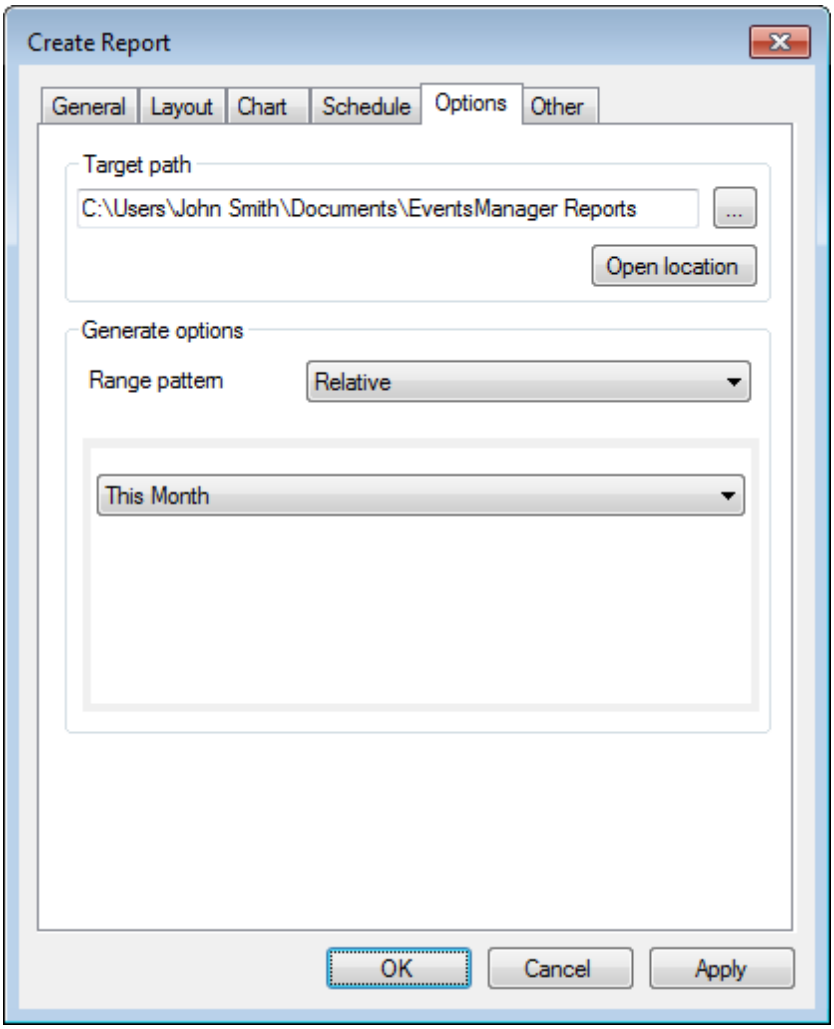
8. Select **Top 10** to view the Top 10 records only.



Screenshot 113: Configuring the schedule for when the report is generated

9. (Optional) Click **Schedule** tab and configure schedule settings.

10. Select **Send report by email to** and click **Configure** to select the recipients of this report.



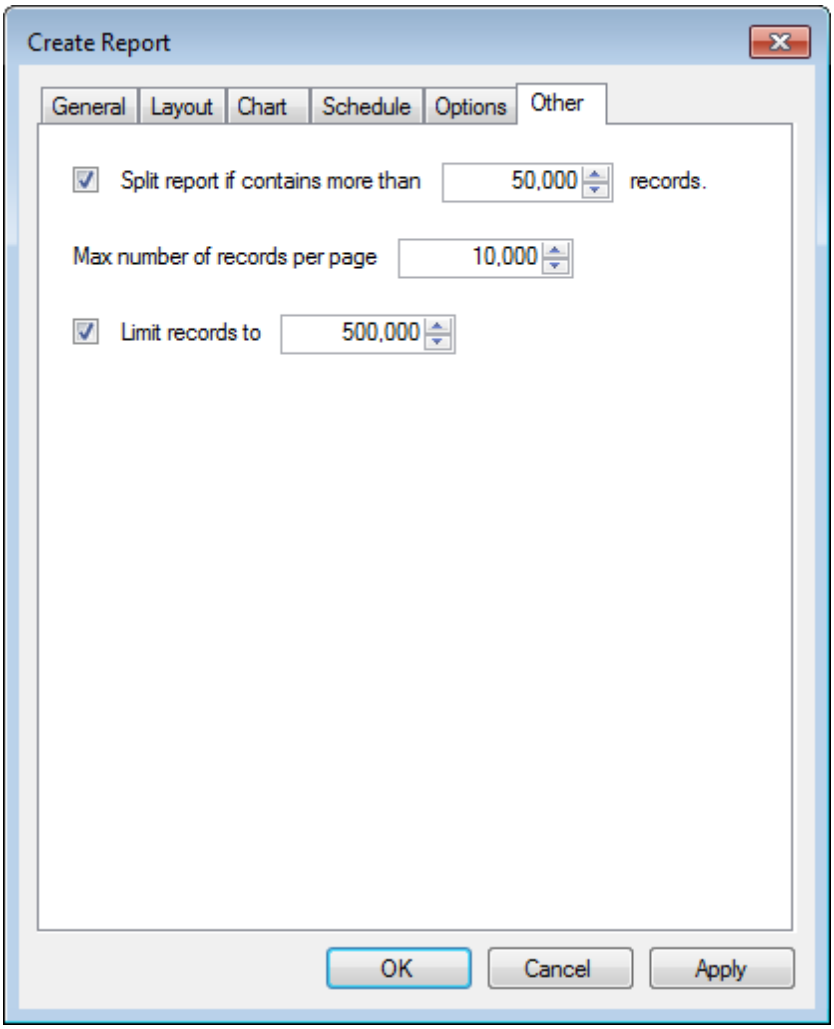
Screenshot 114: Create new report Options

11. Click **Options** tab and specify the path to where the report generates to in the **Target path** area.

12. From the **Range pattern** drop-down menu, select the options described in the table below:

Table 51: Range pattern options

Pattern	Description
All Time	Select **All Time** to generate the report based on information from all the related logs.
Relative	Generate the report based on events from: » Today » Yesterday » Last 7 Days » This Month » Last Month.
Day	Specify a single day that you want to base your report on.
Month	Specify a month and year that you want to base your report on.
Date Range	Specify a **From** and **To** date to base report information on events collected in the specified time period.



Screenshot 115: Record limit settings

13. Click **Other** tab to configure report record limits. Available options are described in the table below:

Table 52: Report record settings

Option	Description
Split report if it contains more than {X} records	Select the checkbox to enable record limit per report. GFI EventsManager automatically creates a new report for every number of records you specify. Example: if you key in 50, 000 and the report contains 150, 000 records, GFI EventsManager generates three reports.
Max number of records per page	Specify the number of records that are displayed in a single page.
Limit records to	Specify the maximum number of records that are included in the report. Records that exceed the limit are ignored.

14. Click **Apply** and **OK**.

8.6 Generating reports

GFI EventsManager enables you to generate a number of different reports, containing information about GFI EventsManager configuration settings, network activity and product activity.

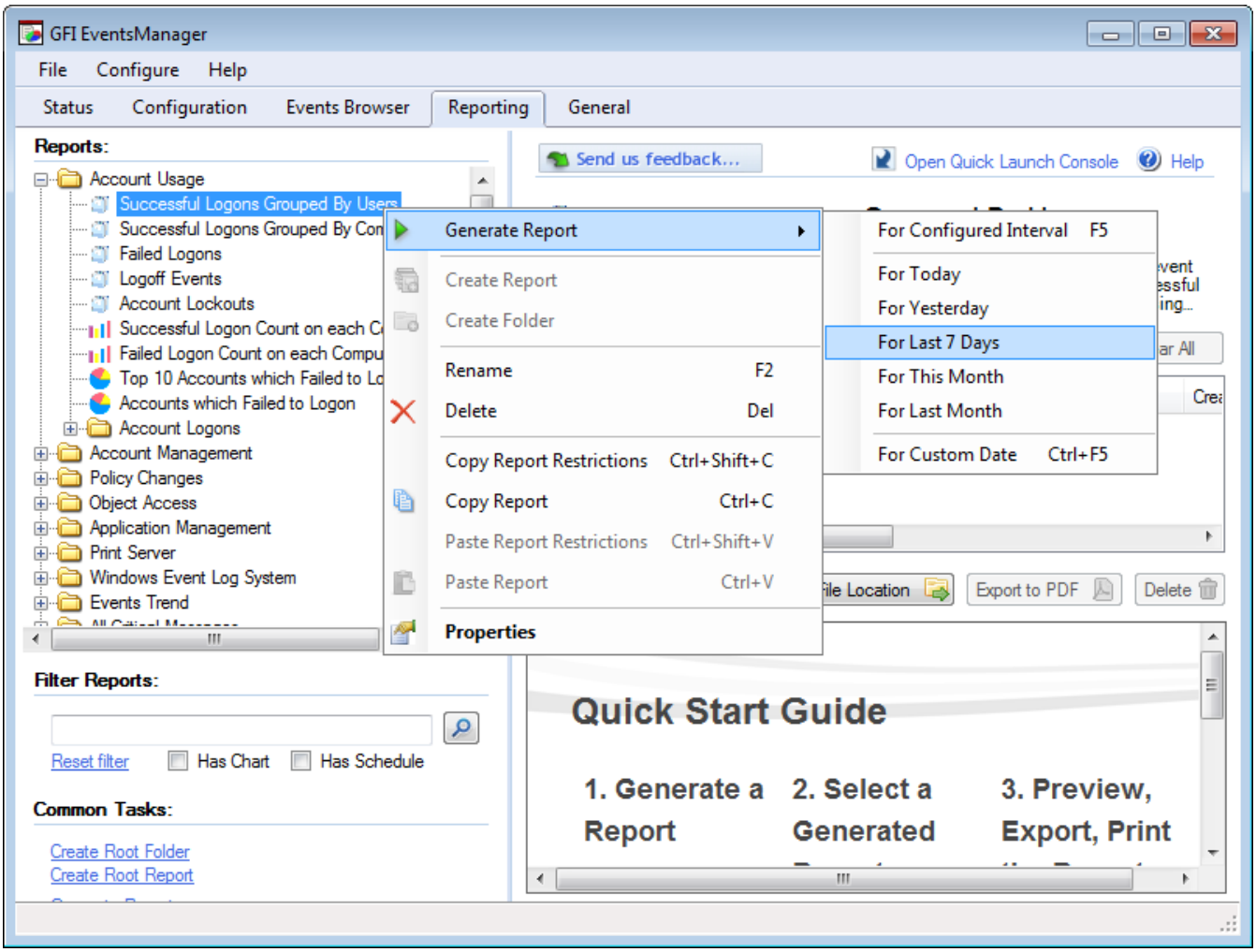
This section contains information about:

- Generating a report
- Generating daily digest reports
- Generating settings reports
- Generating rules reports
- Generating operational history reports
- Generating activity overview reports

8.6.1 Generating a report

To generate a report:

1. From **Reporting** tab > **Reports**, right-click a report and select **Generate Report**.

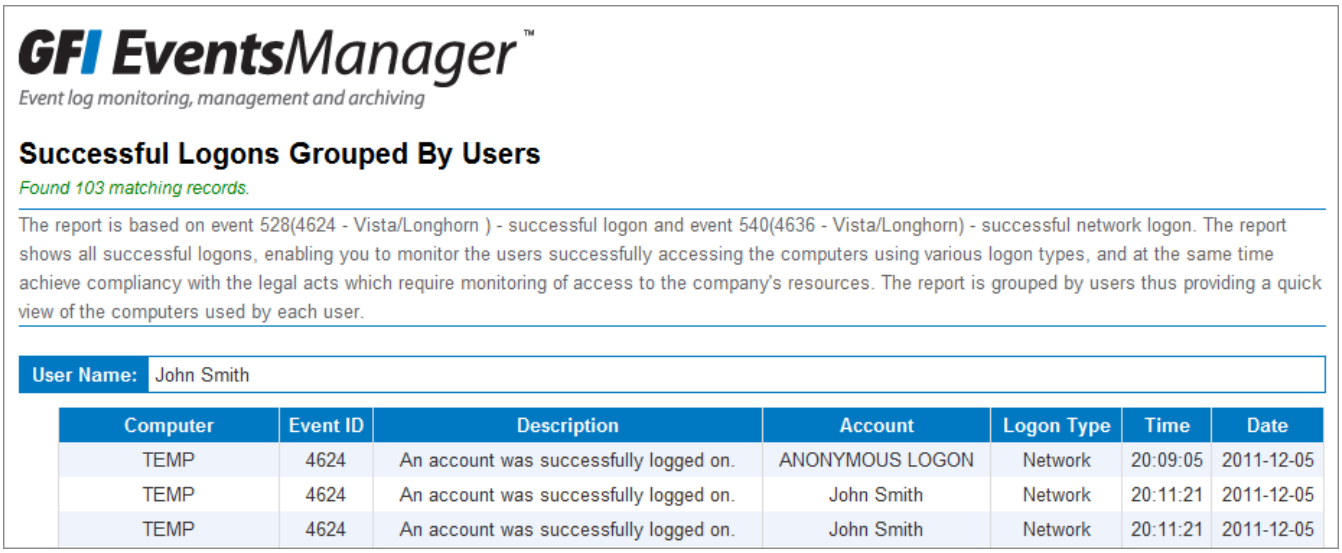


Screenshot 116: Generating a report

2. Wait for the report to generate and view results in **Preview Report** section.

Note

Reports can also be generated by selecting a report from the list and clicking **Generate Report** at the top of the reporting page.



GFI EventsManager™

Event log monitoring, management and archiving

Successful Logons Grouped By Users

Found 103 matching records.

The report is based on event 528(4624 - Vista/Longhorn) - successful logon and event 540(4636 - Vista/Longhorn) - successful network logon. The report shows all successful logons, enabling you to monitor the users successfully accessing the computers using various logon types, and at the same time achieve compliancy with the legal acts which require monitoring of access to the company's resources. The report is grouped by users thus providing a quick view of the computers used by each user.

User Name: John Smith

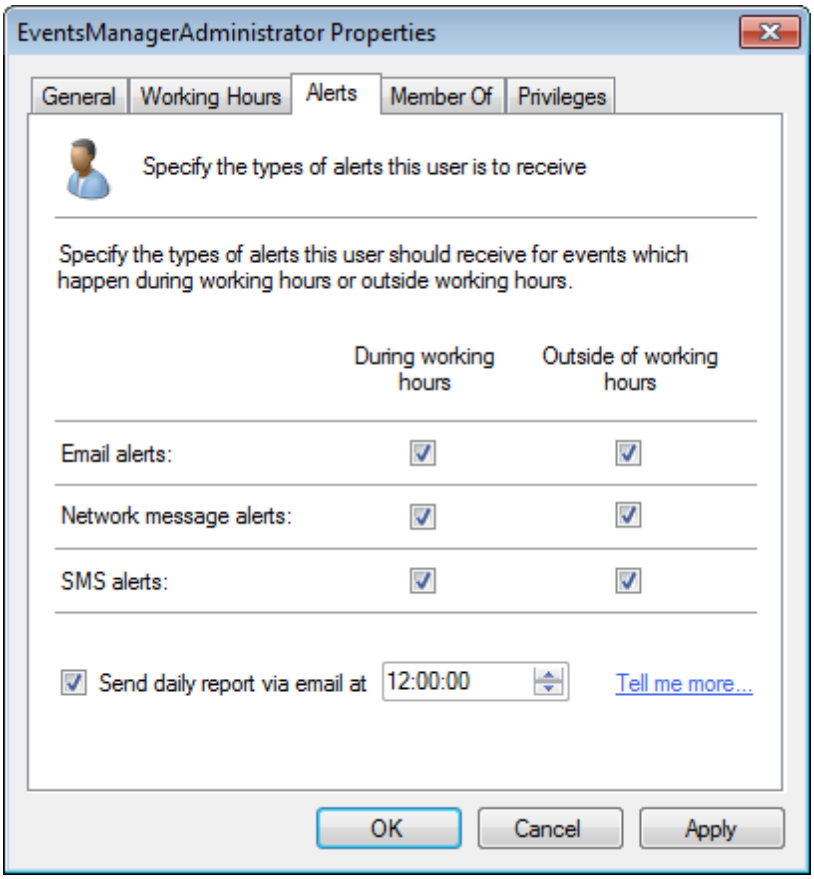
Computer	Event ID	Description	Account	Logon Type	Time	Date
TEMP	4624	An account was successfully logged on.	ANONYMOUS LOGON	Network	20:09:05	2011-12-05
TEMP	4624	An account was successfully logged on.	John Smith	Network	20:11:21	2011-12-05
TEMP	4624	An account was successfully logged on.	John Smith	Network	20:11:21	2011-12-05

Screenshot 117: Report sample

8.6.2 Generating daily digest reports

GFI EventsManager can be configured to send a summary report by email on a daily basis. The report contains a summary of the most important events collected and processed during the last 24 hours. To configure a user to receive Daily Digest emails:

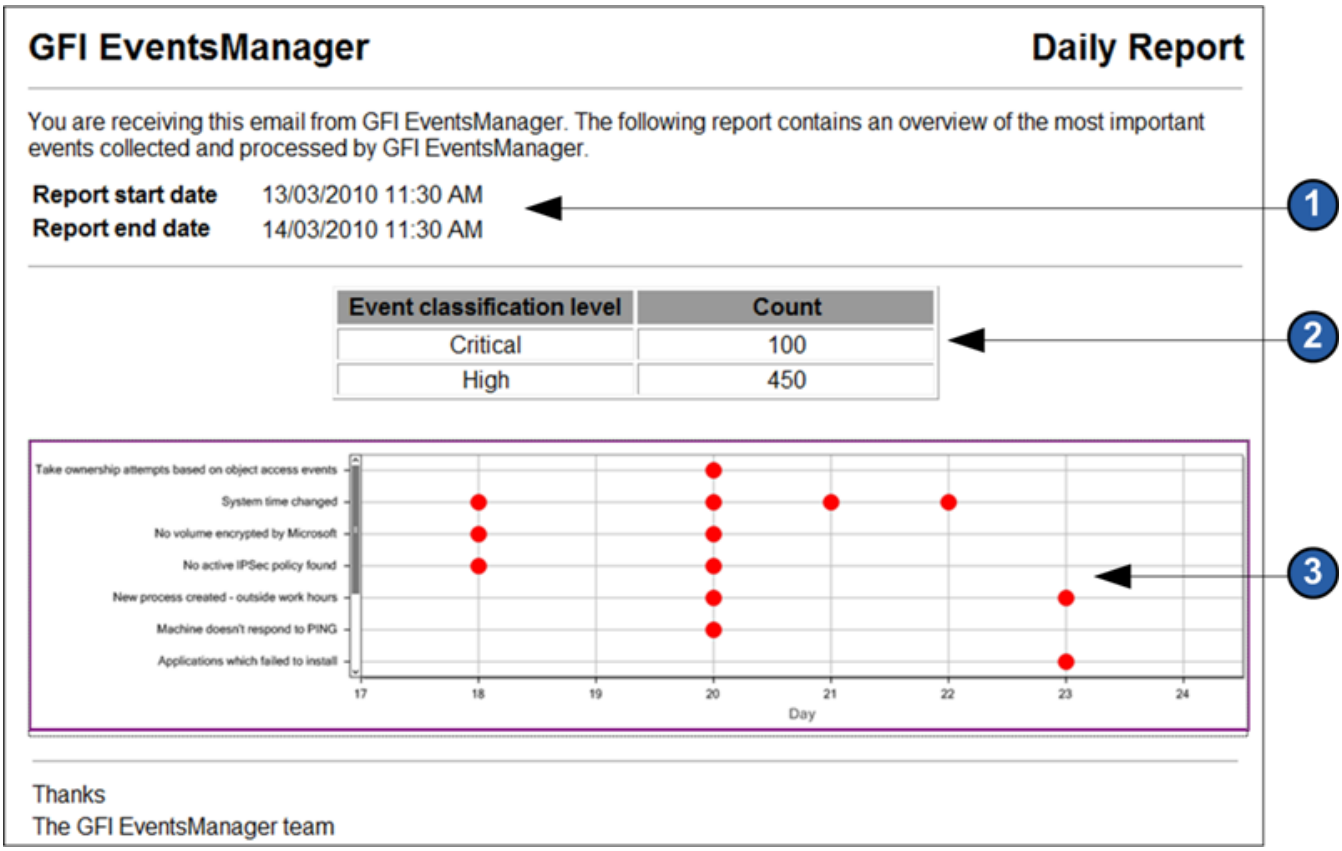
1. From **Configuration** tab > **Options**. Expand **Users and Groups** and select **Users**.
2. Right-click a user from the right pane and select **Properties**.
3. From the **General** tab, ensure that a valid email address is configured.
4. From the **Alerts** tab, select **Send daily report via email**.



Screenshot 118: Daily Digest email settings

5. Configure the time when the Daily Digest email is sent.

6. Click **Apply** and **OK**.



Screenshot 119: Daily digest email

Table 53: Daily digest email description

Section	Description
1	The start and end date of the report. The report displays the most important events collected by GFI EventsManager between the start and end date.
2	The number of Critical and High events collected in the last 24 hours.
3	This graph provides statistical information about critical events collected from all event sources in the last 24 hours.

8.6.3 Generating settings reports

GFI EventsManager enables you to generate settings reports on event source groups. The provided information is described below:

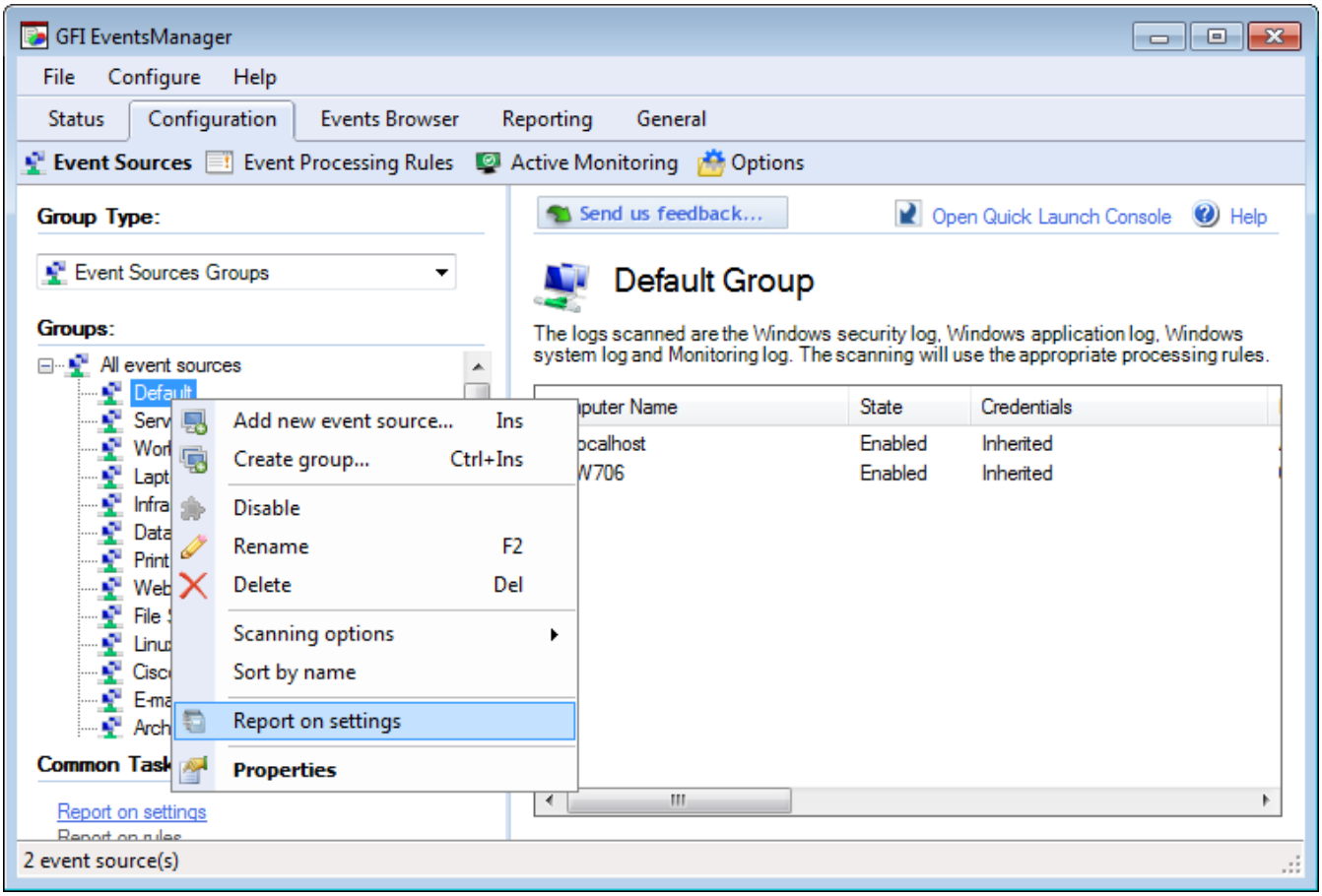
Table 54: Settings report heading information

Heading	Description
Group name	The name of the group the report is based on.
Computer name	A list of every event source in the selected group.
Scan intervals	Scanning interval for every event source in the selected group; shown in **Days : Hours : Minutes : Seconds**.

Heading	Description
Rules folder	Provides a list of rule categories applied to the selected group, such as: » Noise reduction » Security » System health » PCI DSS requirements.
Rule sets	A granular list of rules applied on the selected group.

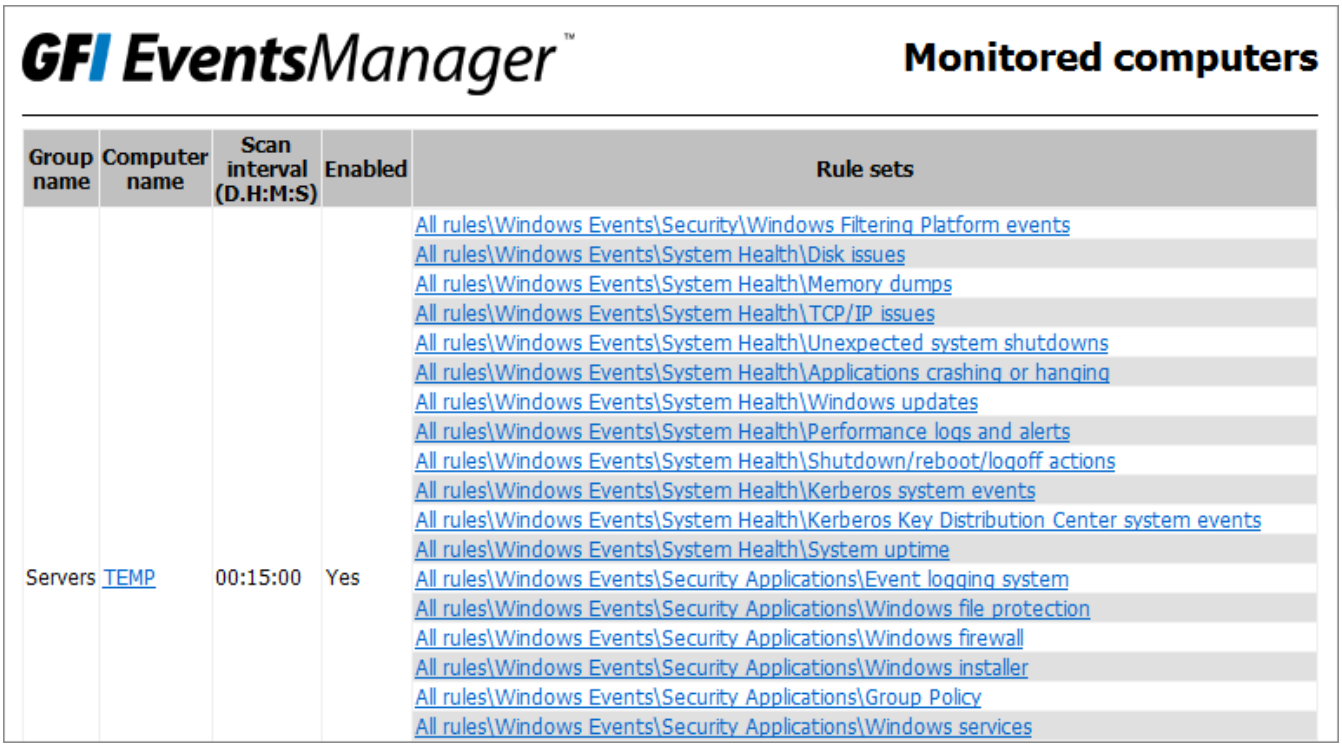
To generate settings report:

1. Click **Configuration** tab > **Event Sources**.



Screenshot 120: Generate configuration report

2. Right-click an event source group and select **Report on settings**.



GFI EventsManager™ **Monitored computers**

Group name	Computer name	Scan interval (D.H:M:S)	Enabled	Rule sets
Servers	TEMP	00:15:00	Yes	All rules\Windows Events\Security\Windows Filtering Platform events All rules\Windows Events\System Health\Disk issues All rules\Windows Events\System Health\Memory dumps All rules\Windows Events\System Health\TCP/IP issues All rules\Windows Events\System Health\Unexpected system shutdowns All rules\Windows Events\System Health\Applications crashing or hanging All rules\Windows Events\System Health\Windows updates All rules\Windows Events\System Health\Performance logs and alerts All rules\Windows Events\System Health\Shutdown/reboot/logoff actions All rules\Windows Events\System Health\Kerberos system events All rules\Windows Events\System Health\Kerberos Key Distribution Center system events All rules\Windows Events\System Health\System uptime All rules\Windows Events\Security Applications\Event logging system All rules\Windows Events\Security Applications\Windows file protection All rules\Windows Events\Security Applications\Windows firewall All rules\Windows Events\Security Applications\Windows installer All rules\Windows Events\Security Applications\Group Policy All rules\Windows Events\Security Applications\Windows services

Screenshot 121: Settings report sample

8.6.4 Generating rules reports

Rules repots provide a detailed view of applied rules on event sources. The information provided in rules reports are described below:

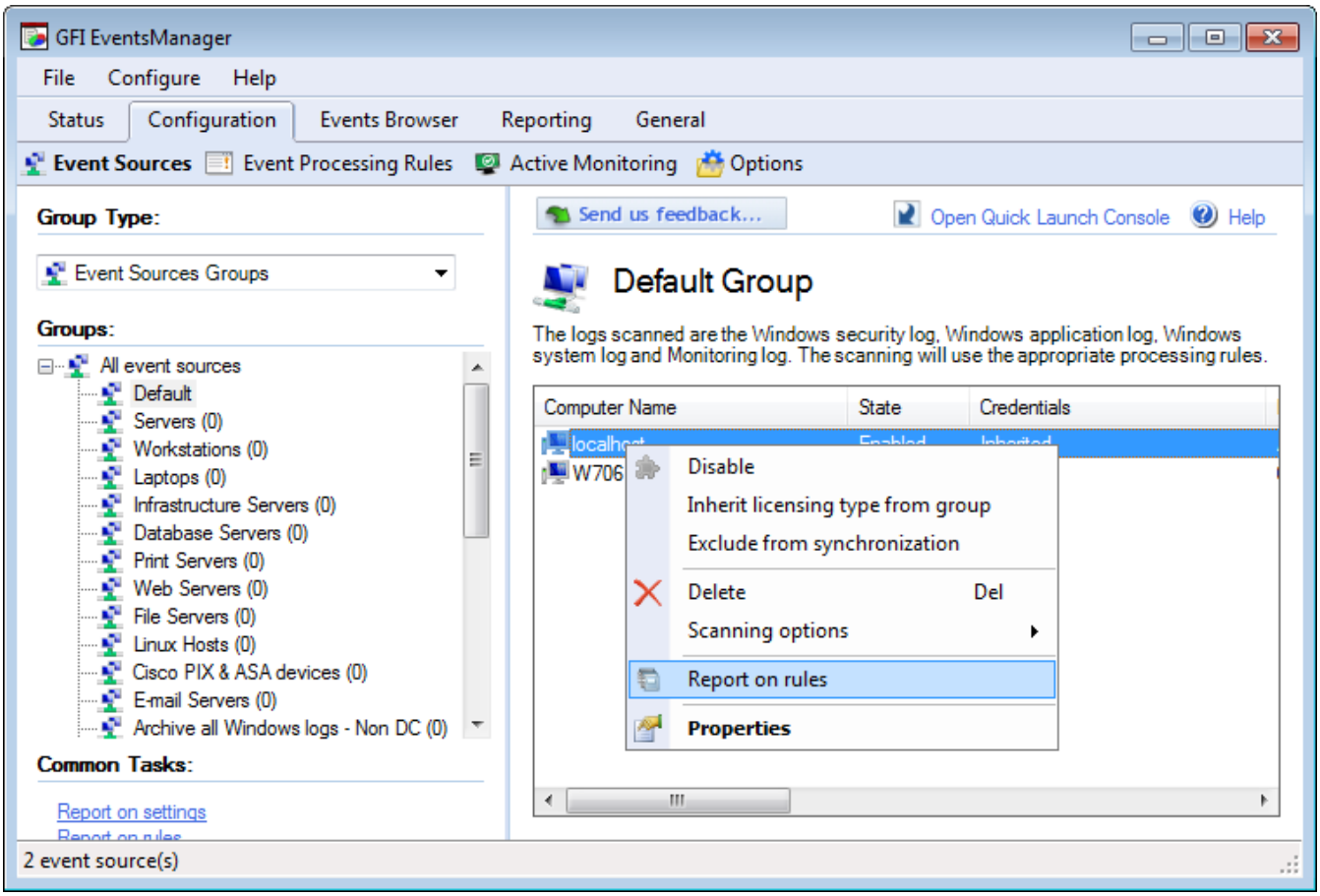
Table 55: Rules report heading information

Heading	Description
Rule name	Name of the applied rule.
Importance	The classified importance level of the collect event log, such as: » Critical » High » Medium » Low » Noise event.
Logfile monitored	Provides the category name of the collected event log, such as: » Security » System Health » Application » System.
Conditions	The processing condition(s) for the selected rule. This includes: » Event IDs » Source » Category » User » Type » Advanced.

Heading	Description
Actions	Describes the actions taken when the event is processed, including: » Archiving settings » Mail to settings » Threshold settings.

To generate rules report:

1. Click **Configuration** tab > **Event Sources**.



Screenshot 122: Generate configuration report

2. Right-click an event source and select **Report on rules**.

8.6.5 Generating operational history reports

GFI EventsManager's operational history can be exported for further analysis and archiving purposes. Operational history messages provide administrators with information as described below:

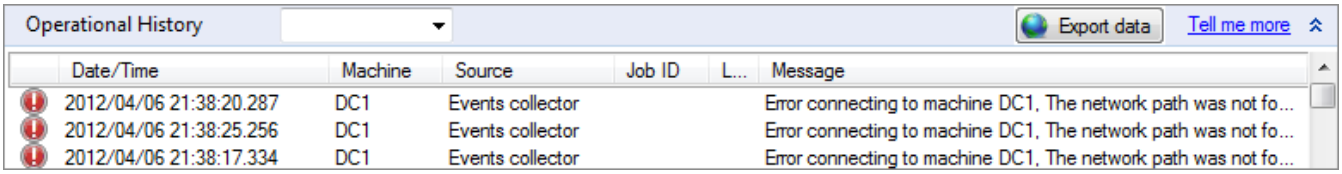
Table 56: Operational History report description

Date/Time	Date and time when the message was generated.
Machine	Event source that generated the message.
Source	Source operation that cause the message to be generated. Amongst others these include: » **EvtCollector** - message generated while collecting event logs » **SNMP TrapsServer** - message generated while collecting SNMP Traps Messages » **EnetrpriseMaintenance** - message generated during database maintenance jobs.
Job ID	An internal ID associated with the job.

Log file/name	Type of logs collected. Amongst others: Application Security Logs generated by other applications such as GFI LanGuard and GFI EndPointSecurity.
Message	The actual message generated while performing the job.

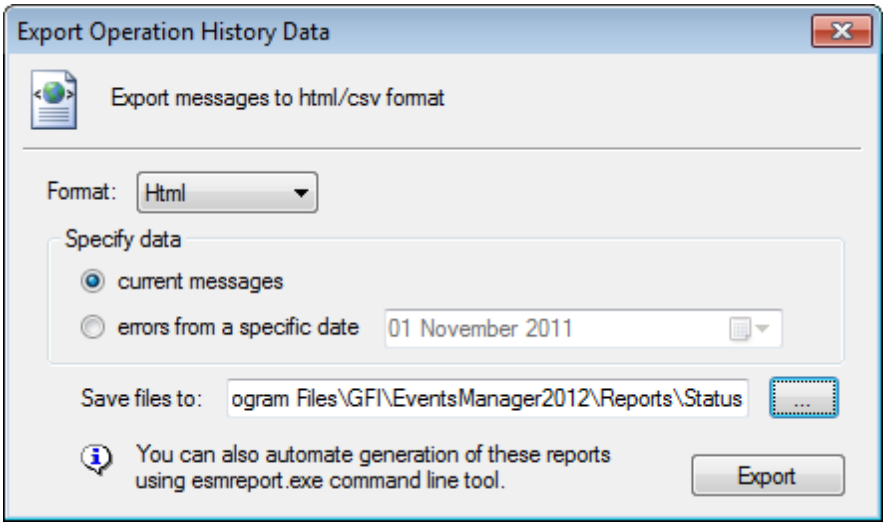
To generate Operational History reports:

1. Click **Status** tab > **Job Activity**.



Screenshot 123: Operational History report

2. Click **Export data**.



Screenshot 124: Operational History dialog

3. Specify the options described below and click **Export**.

Table 57: Operational History export options

Option	Description
Format	Select the report output format. Available formats are HTML and CSV.
Current messages	Export all messages displayed in Job Activity tab.
Errors from a specific date	Specify a date and export all the messages generated on that date.
Save file to	Select checkbox to specify output location. If not selected, reports are saved in the default location within the GFI EventsManager directory.

GFI EventsManager

Operational History for period: 2011-11-01

Date/Time	Type	Machine	Source	Job ID	Log file/name	Message
31/10/2011 18:41:03	Information	192.168.3.1	EvtCollector	N/A	GFI EventsManager	Start executing checks on machine 192.168.3.1..
31/10/2011 18:41:04	Information	192.168.3.1	EvtCollector	N/A	GFI EventsManager	Executed 5 checks on machine 192.168.3.1
31/10/2011 18:41:04	Information	192.168.3.1	EvtCollector	B3789E4A	Security	Start the collection on machine 192.168.3.1, log Security
31/10/2011 18:41:30	Information	192.168.3.1	ProcessorService	N/A	windows	Processing 2000 windows events from machine 192.168.3.1.
31/10/2011 18:41:33	Information	192.168.3.1	EvtCollector	1017473C	Application	Start the collection on machine 192.168.3.1, log Application
31/10/2011 18:41:45	Information	192.168.3.1	ProcessorService	N/A	windows	Processing 2000 windows events from machine 192.168.3.1.

Screenshot 125: Operational History report sample

8.6.6 Generating activity overview reports

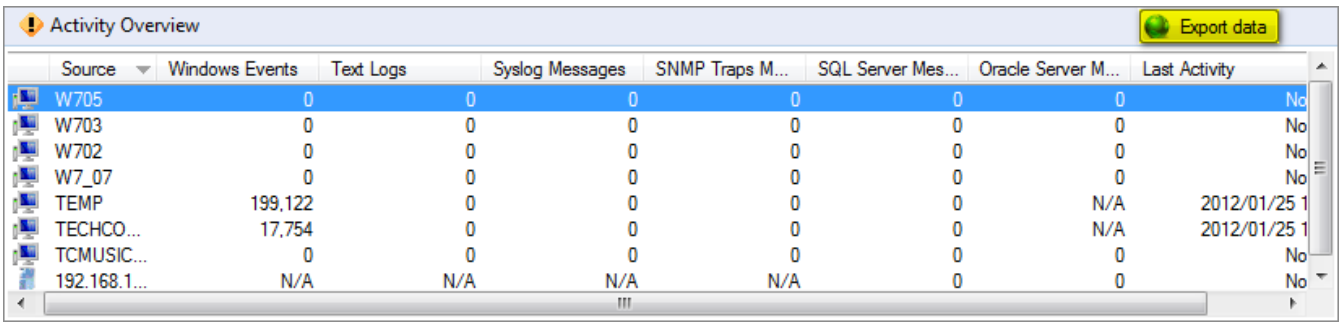
GFI EventsManager enables you to export Activity Overview data. Activity overview reports provide the information described below:

Table 58: Activity overview report headings

Heading	Description
Date/Time	Date and time when the message was generated.
Machine	Event source that generated the message.
Source	Source operation that cause the message to be generated. Amongst others these include: » **EvtCollector** - message generated while collecting event logs » **SNMP Traps Server** - message generated while collecting SNMP Traps Messages » **EnetrpriseMaintenance** - message generated during database maintenance jobs.
Job ID	An internal ID associated with the job.
Log file/name	Type of logs collected. Amongst others: » Application » Security » Logs generated by other applications such as GFI LanGuard and GFI EndPointSecurity
Message	The actual message generated while performing the job.

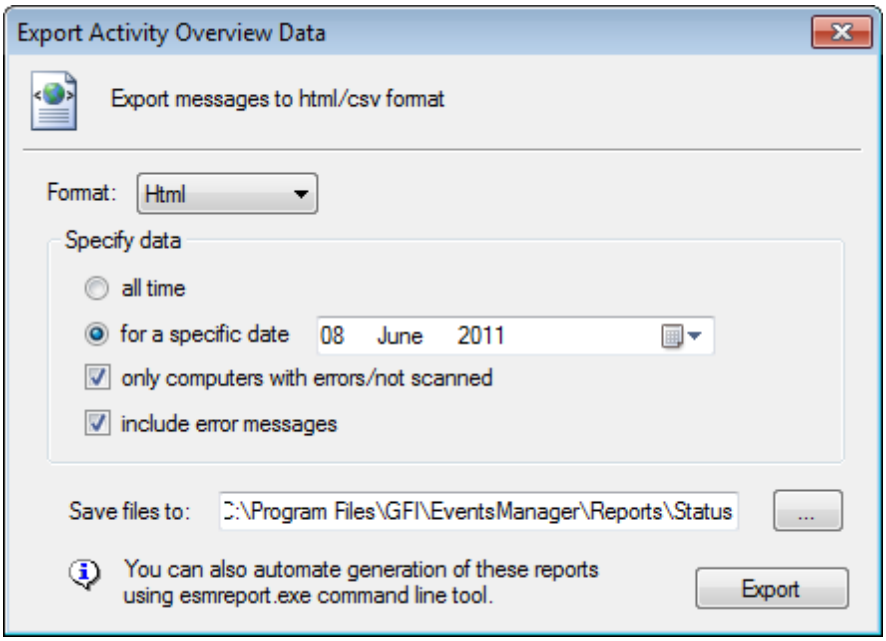
To export Activity Overview:

1. Click **Status > Statistics**.


Activity Overview
Export data
Source
Windows Events
Text Logs
Syslog Messages
SNMP Traps M...
SQL Server Mes...
Oracle Server M...
Last Activity
W705 0 0 0 0 0 0 No
W703 0 0 0 0 0 0 No
W702 0 0 0 0 0 0 No
W7_07 0 0 0 0 0 0 No
TEMP 199,122 0 0 0 0 N/A 2012/01/25 1
TECHCO... 17,754 0 0 0 0 N/A 2012/01/25 1
TCMUSIC... 0 0 0 0 0 0 No
192.168.1... N/A N/A N/A N/A 0 0 No

Screenshot 126: Activity overview : Export button

2. Click **Export data**.



Screenshot 127: Activity overview dialog

3. Configure the options described in and click **Export**.

Table 59: Export Operational History options

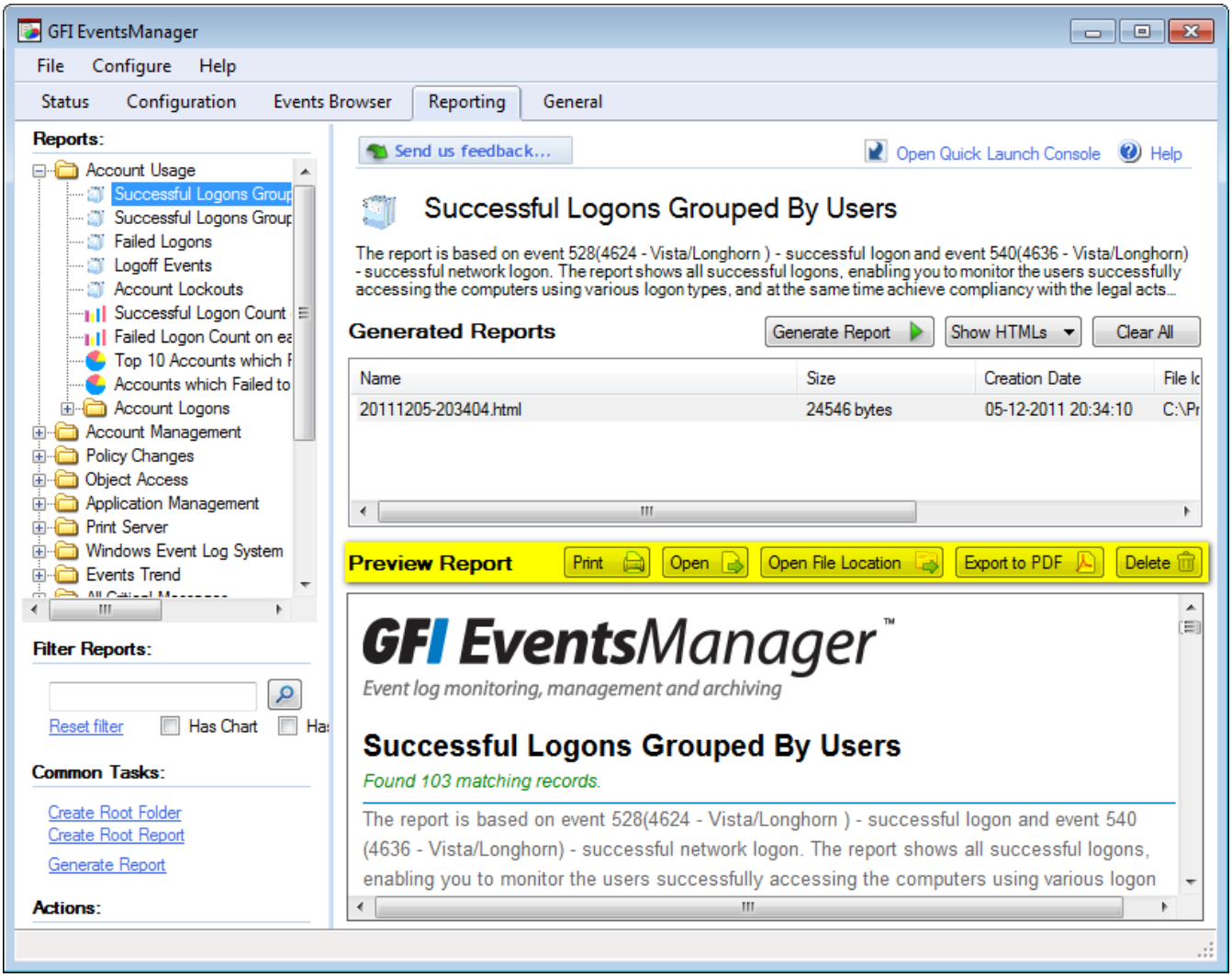
Option	Description
Format	The report output format. Available formats are HTML and CSV.
All time	Export all messages displayed Activity Overview.
From a specific date	Specify a date to export all messages generated on that date.
Only computers with errors/not scanned	Export only data of computers with scanning issues.
Include error messages	Select this option to include the generated error message.
Save files to	Displays the default export location.

GFI EventsManager™ **Activity Overview for period: 2012/01/25**

Source	Windows Events	Text Logs Events	Syslog Messages	SNMP Traps Messages	SQL Server Messages	Oracle Server Messages	Last Activity
TCMUSICSERVER	0	N/A	N/A	N/A	N/A	N/A	No Activity
TECHCOMSERVTWO	23753	N/A	N/A	N/A	N/A	N/A	2012/01/25 18:08:00.933
TEMP	196799	N/A	N/A	N/A	N/A	N/A	2012/01/25 17:55:47.542
W7_07	0	N/A	N/A	N/A	N/A	N/A	No Activity
W702	0	N/A	N/A	N/A	N/A	N/A	No Activity
W703	0	N/A	N/A	N/A	N/A	N/A	No Activity
W705	0	N/A	N/A	N/A	N/A	N/A	No Activity
192.168.11.11	N/A	N/A	N/A	N/A	N/A	0	No Activity

Screenshot 128: Activity overview report sample

8.7 Analyzing reports



Screenshot 129: Analyzing reports

The reporting system of GFI EventsManager comes with dedicated tools to help you analyze and export reports. Once a report is generated, select it from the list of Generated Reports and use the common controls which help you run common report analysis commands. The available tools are described below:

Table 60: Analyzing reports: Tools

Option	Description
Print	Use the **Print** option to view a print preview, configure printer settings and print the selected report.
Open	Use the **Open** button to open the selected report in a browser. GFI EventsManager uses your default browser to view reports in HTML.
Open File Location	**Open File Location** enables you access the folder containing the report for backup or archiving purposes.
Export to PDF	Use **Export to PDF** to export the selected report to Portable Document Format.
Delete	Click **Delete** to remove a generated report from the list.

8.8 Defining column headings

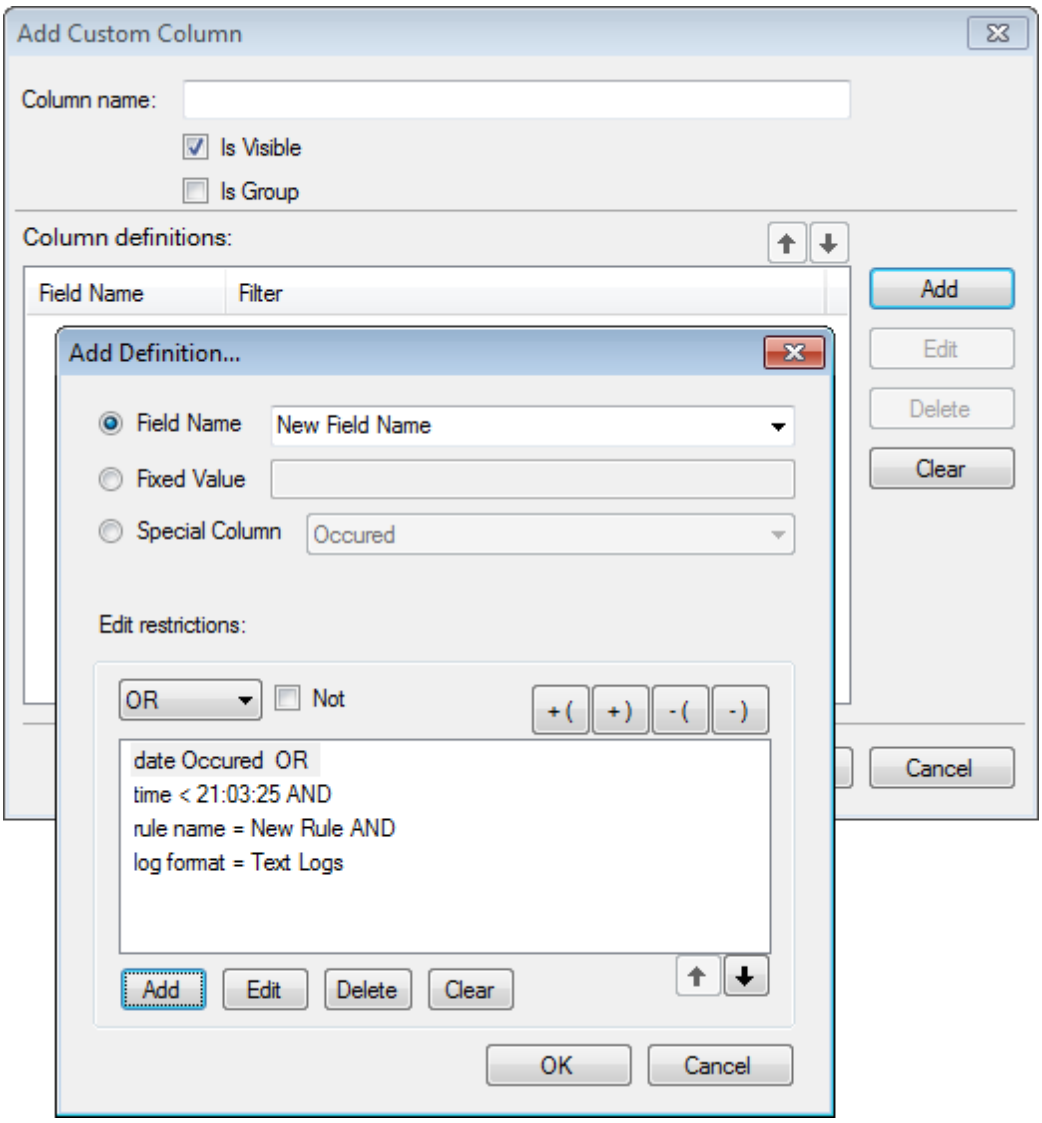
GFI EventsManager enables you to create custom columns through the **Add Custom Columns** dialog. This dialog allows you specify conditions, create a new field and add them to your report(s). Also based on conditions, this dialog enables you to further customize existing or new reports.

To add custom columns:

1. From **Reporting** tab **>** **Actions**, click **Create Report**.

2. Click **Layout** tab **>** **Add Existing Column**, to add default columns.

3. Click **Add Custom Column** to launch the **Add Custom Columns** dialog.



Screenshot 130: Define custom column conditions

4. From the **Add Custom Column** dialog click **Add**.

5. From the **Add Definition…** dialog, configure the options described below:

Table 61: Add Column Definition options

Option	Description
Field Name	Specify a name for the new field.

Option	Description
Fixed Value	Select **Fixed Value** if the value of the new field is going to be fixed. Specify a value as a field name. For example, to check that events always occur after 5pm, specify 5 as the fixed value instead of defining a time field and assign a value of 5.
Special Column	Special columns are predefined columns that may be used in your condition.
Edit restrictions	This section enables you to add, edit or delete field restrictions.

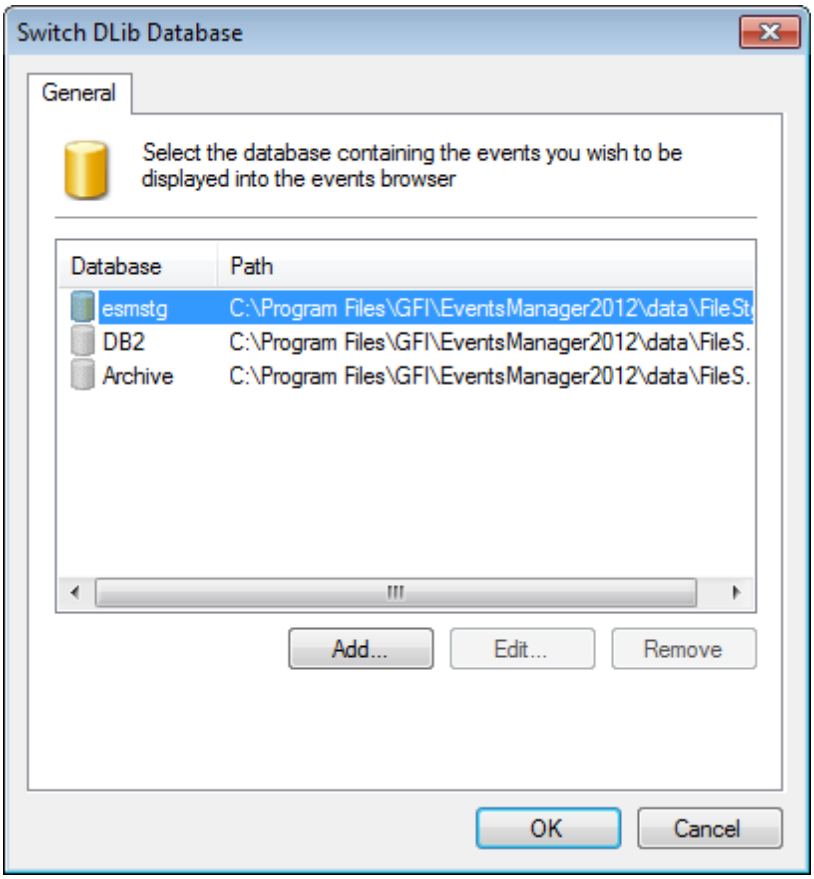
6. Click **Apply** and **OK**.

8.8.1 Reporting on events from different databases

For reporting purposes, GFI EventsManager enables you to switch between different databases. Use this feature to report on events that have been exported/archived for further analysis or stored in different databases.

To switch database:

1. From **Reports** tab > **Common Tasks**, click **Switch database**.



Screenshot 131: Switch database dialog

2. Select the database from the list of databases and click **OK**. Click **Add…** to specify a new database name and it's relevant path. Click **Edit…** to edit the specified information.

8.9 Customizing HTML reports

HTML report templates are customizable, enabling you to further tweak GFI EventsManager to suit your daily requirements. To edit the available templates, knowledge of HTML and CSS is required.

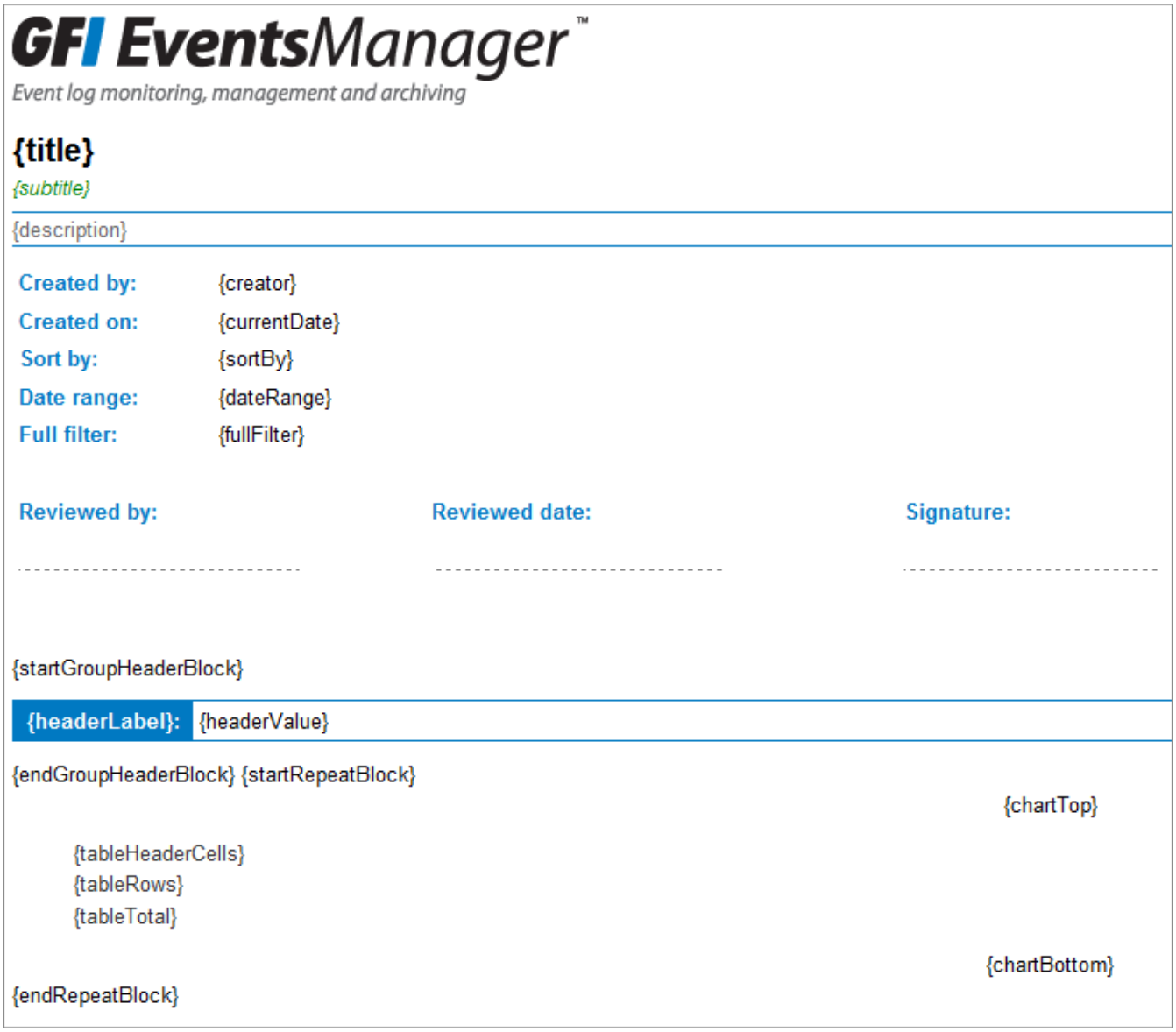
Important

Before editing the default report template, save a copy of the original so that you can easily revert to default for troubleshooting.

To edit the layout of HTML reports:

1. Go to GFI EventsManager install directory:

```
%Program Files\GFI\EventsManager2012\Data\Templates\DefaultReportLayout
```



Screenshot 132: Editing HTML report templates

2. From **DefaultReportLayout** folder, edit the templates described below:

Table 62: Default HTML templates

Template	Description
template_group_new.html	This template is used when generating reports which contain data about grouped sources. Grouping can be by users, sources, event data and more.
template_new.html	Use this template to generate statistical and graphical reports which do not organize data into groups.

3. Using an HTML editor, edit the following elements of the templates:

Table 63: HTML template: Editable sections

Section	Description
Report logo	Replace GFI EventsManager logo with a logo of your choice. Add more logos or completely remove them from your reports.
Labels and text	Rename and reposition labels according to your needs.
Placeholders	Although you are able to move placeholders around the report, renaming them will cause GFI Events-Manager reporting engine to fail to return the respective data.

Available placeholders include:

Table 64: HTML report template placeholders

Placeholder	Description
{title}	Title of report.
{subtitle}	Subtitle of report.
{description}	Description of report.
{creator}	User who generated report.
{currentDate}	Date when report is generated.
{sortBy}	Sort field.
{dateRange}	Report data is gathered from the specified time period.
{fullFilter}	List of Restrictions set for the Report.
{startGroupHeaderBlock}	Beginning of Header section of the repetitive block.
{headerLabel}	Name of grouping header.
{headerValue}	Value of grouping header.
{endGroupHeaderBlock}	Ending of Header section of the repetitive block.
{startRepeatBlock}	Beginning of the Body section of the repetitive block.
{tableHeaderCells}	The Header section of the table data.
{tableRows}	The Body section of the table data.
{tableTotal}	For charts. Contains the Sum or Count value of the computed field.
{chartTop}	Places the chart at the beginning of the report.
{chartBottom}	Places the chart at the end of the report.
{endRepeateBlock}	Ending of the Body section of the repetitive block.

4. Save the HTML template and generate a report using the new layout. For more information, refer to Generating reports (page 158).

Note

Using the same HTML/CSS conventions of the HTML templates, you are also able to create your own customized templates. Copy the template, rename it and reuse the same placeholders.

9 Events Processing Rules

During events processing, GFI EventsManager runs a configurable set of rules against the collected logs in order to classify events and trigger alerts/actions accordingly. By default, GFI EventsManager ships with a pre-configured set of events processing rules that allow you to gain network-wide control over computer logs - with negligible configuration effort. You can also customize these default rules or create tailored ones for your organization's requirements.

Topics in this chapter:

9.1 About events processing rules 173

9.2 Managing rules-set folders 175

9.3 Creating new events processing rules 178

9.4 Creating new rules from existing events 183

9.5 Advanced event filtering parameters 188

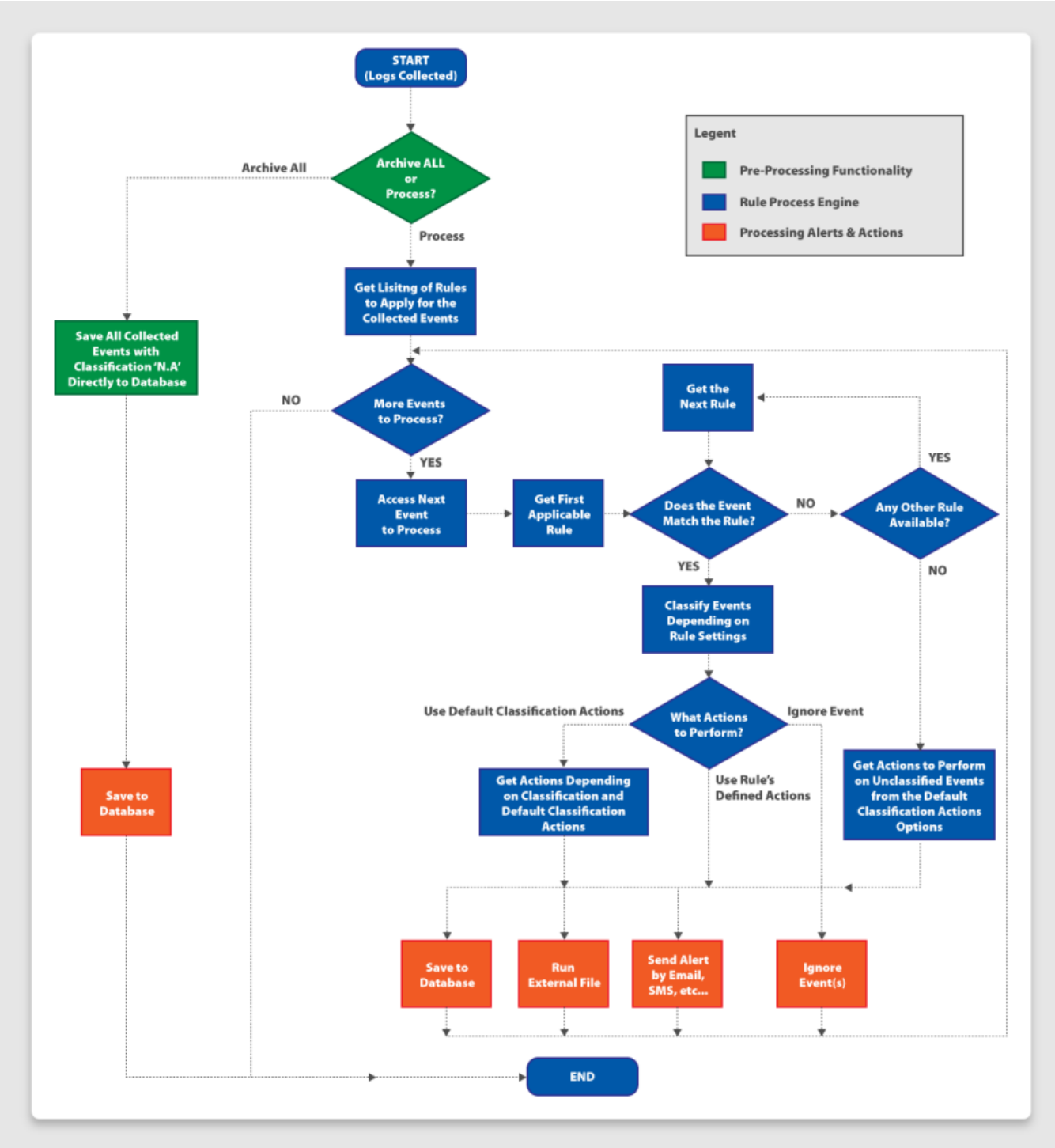
9.6 Prioritizing events processing rules 189

9.1 About events processing rules

Events processing rules are checks that are run against event logs when they are collected. Based on the conditions configured in a rule, events processing rules help you:

- **Classify processed events** - assign a severity rating to collected logs. This enables you to trigger actions or notifications if a certain severity log is processed. By default, events are classified using five main ratings, however, more ratings can be added
- **Filter out noise (repeated events) or unwanted events** - remove duplicate logs or logs that are not important for you and archive important event data only. This reduces database growth and saves storage space
- **Trigger Email, SMS and Network alerts on key events** - send notifications to configured recipients upon detection of certain events. You can configure an event processing rule to send notifications to recipients when the rule conditions are met
- **Attempt remedial actions** - run executable files, commands and scripts upon detection of specific events. This enables you to automatically perform remedial actions to mitigate or completely eliminate a detected problem
- **Filter events that match specific criteria** - remove event logs that are not important for you. Example, you can run a rule which filters out low severity or duplicate events
- **Archive filtered events** - event archiving is based on the severity of the event and on the configuration settings of the event processing rules. Example: you can configure GFI EventsManager to archive only events that are classified as critical or high in severity and discard all the rest.

The flowchart chart below illustrates the event processing stages performed by GFI EventsManager:



Screenshot 133: How Events Processing Rules work

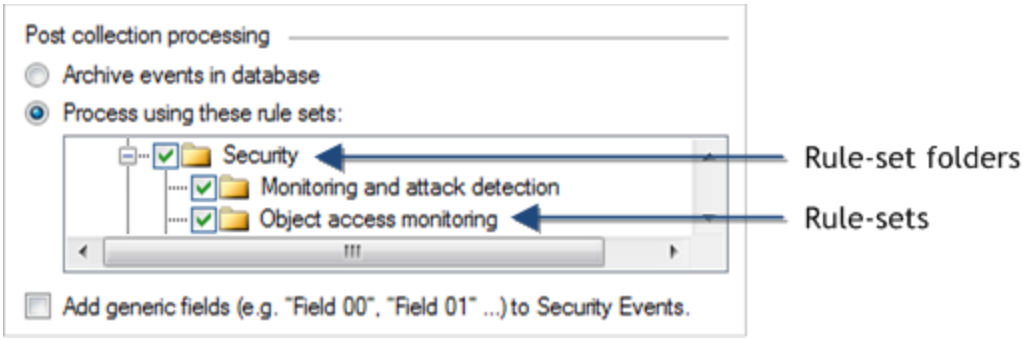
9.1.1 Event classification

Event classification is based on the configuration of the rules that are executed against the collected logs. Events that don't satisfy any event classification conditions are tagged as unclassified. Unclassified events may also be used to trigger the same alerts and actions available for classified events.

GFI EventsManager classifies events in the standard importance levels such as Critical, High, Medium, Low and Noise (unwanted or repeated log entries).

9.2 Managing rules-set folders

In GFI EventsManager, event processing rules are organized into rule-sets and every rule-set can contain one or more specialized rules which can be run against collected logs.



Screenshot 134: Rule-sets folder and Rule-sets

Rule-sets are further organized into Rule-set Folders. This way you can group rule-sets according to the functions and actions that the respective rules perform. By default, GFI EventsManager ships with pre-configured folders, rule-sets and event processing rules that can be further customized to suite your event processing requirements.

This topic contains information about:

- Available rule-sets
- Adding a rule-set folder
- Renaming and Deleting rule-set folders

9.2.1 Available rule-sets

The following table provides you with the available rules-set folders available when you install GFI EventsManager. Each rule-set folder contains multiple rule-sets and/or events processing rules:

Table 65: Common available rule-set folders

Rule-Set Folder	Description
Windows Events	Contains rules tailored for Windows® servers and workstations; These include: » Noise reduction rules » PCI DSS Requirements rules » Security rules » System Health rules » Security Application rules » Infrastructure Server rules » Database Server rules » Web Server rules » Print Server rules » GFI rules » Terminal Services rules » Email Server rules » File Replication rules » Directory Service rules » Custom rules » Reporting rules » SharePoint Audit rules.
Text Logs	Contains rules tailored for the processing of web transfer protocols. These include: » HTTP rules » FTP rules » SMTP rules.
Syslog Messages	Contains rules tailored for the processing LINUX and UNIX system logs. These include: » Linux\Unix hosts rules » Juniper Networks rules » Cisco PIX and ISA rules » Rules by severity » IBM iSeries rules.
SNMP Traps	Contains rules tailored for SNMP Traps Messaging. These include: » Cisco IOS release 12.1 (11) MIBs rules » Cisco IOS release 12.1 (14) MIBs rules » Cisco IOS release 12.2 (20) MIBs rules » Cisco IOS release 12.2 (25) MIBs rules » Allied Telesis AT-AR-700 Family rules.

Rule-Set Folder	Description
SQL Server® Audits	Contains rules tailored for SQL Server® Audit monitoring. These include: » Noise reduction rules » Database changes rules » Server changes rules » Logon/Logoff rules » SQL Server® rules » Database access rules.
Oracle Audits	Contains rules tailored for Oracle Server Audit monitoring. Amongst others, these include: » Noise reduction rules » Database changes rules » Server changes rules » Logon/Logoff rules » Security changes rules.
Monitoring Checks	Contains rules that enable you to monitor active monitoring messages. These include rules pertaining to the default set of monitoring checks. Monitoring checks generate event logs. These event logs can be processed by events processing rules to trigger an action or notification when a fault is detected.

9.2.2 Adding a rule-set folder

To create a new rule-set folder:

1. Click **Configuration** tab and select **Event Processing Rules**.
2. From **Common Tasks**, select **Create folder**.
3. Specify a unique name for the new rule-set folder.

> **Note**
>
> To create sub rule-set folders, right-click on the parent folder and select **Create new folder…**

9.2.3 Renaming and Deleting a rule-set folder

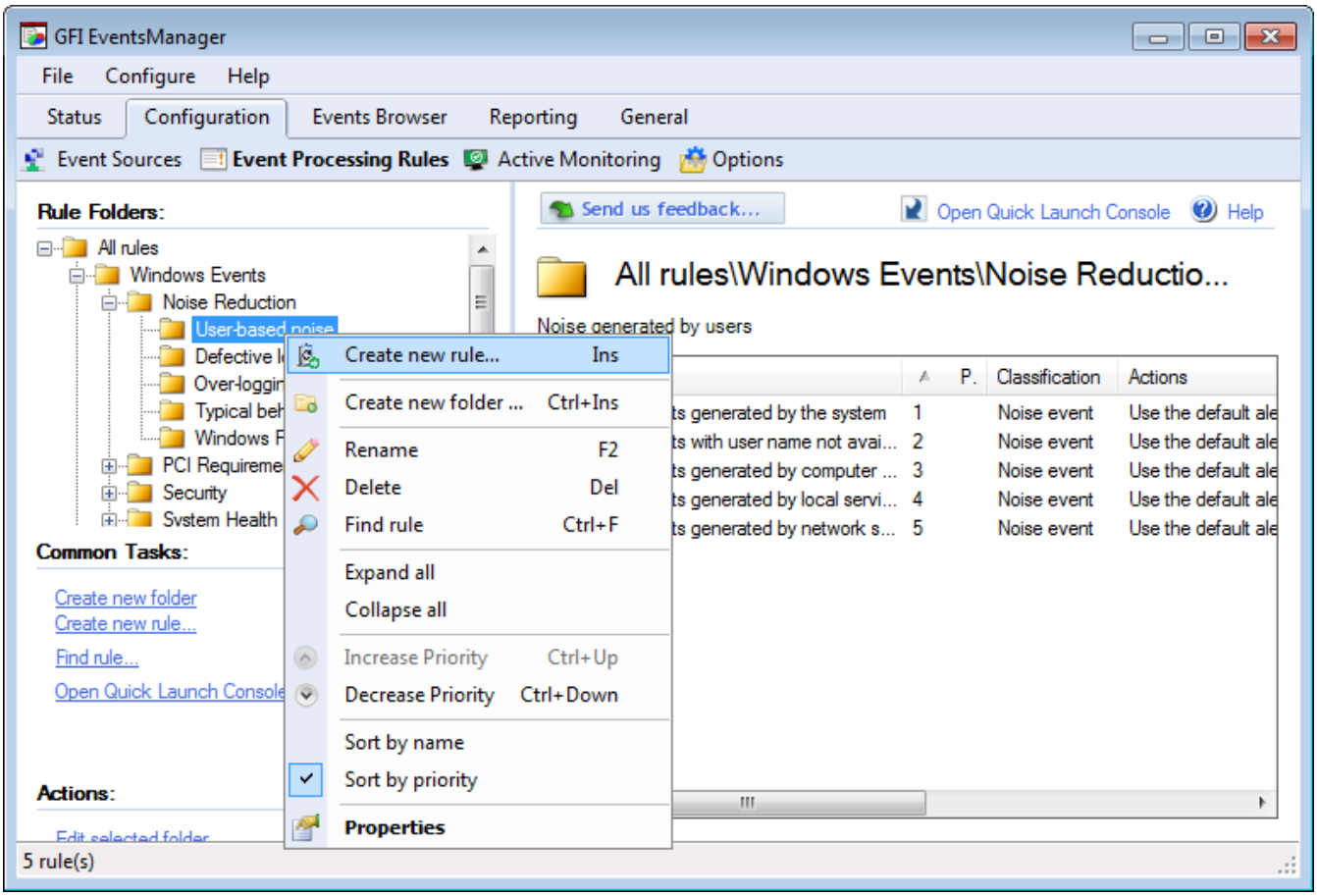
To rename or delete existing rule-set folders, right-click on the target rule-set folder and select **Rename** or **Delete** accordingly.

> **Important**
>
> Deleting a rule-set folder will lead to the deletion of all the rules and rule-sets contained within the deleted folder.

9.3 Creating new events processing rules

To create a new event processing rule:

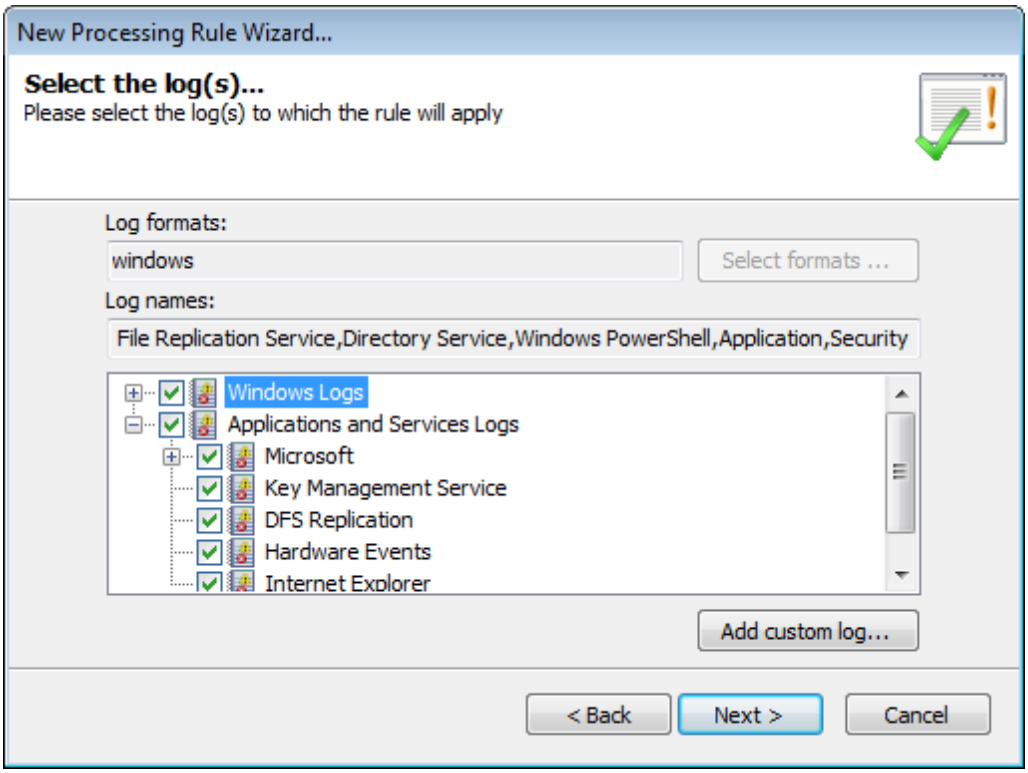
1. Click **Configuration** tab > **Event Processing Rules**.



Screenshot 135: Creating a new rule

2. Right-click the rule-set where the new rule will be created and click **Create new rule...**

3. Specify the name and description (optional) for the new rule. Click **Next**.



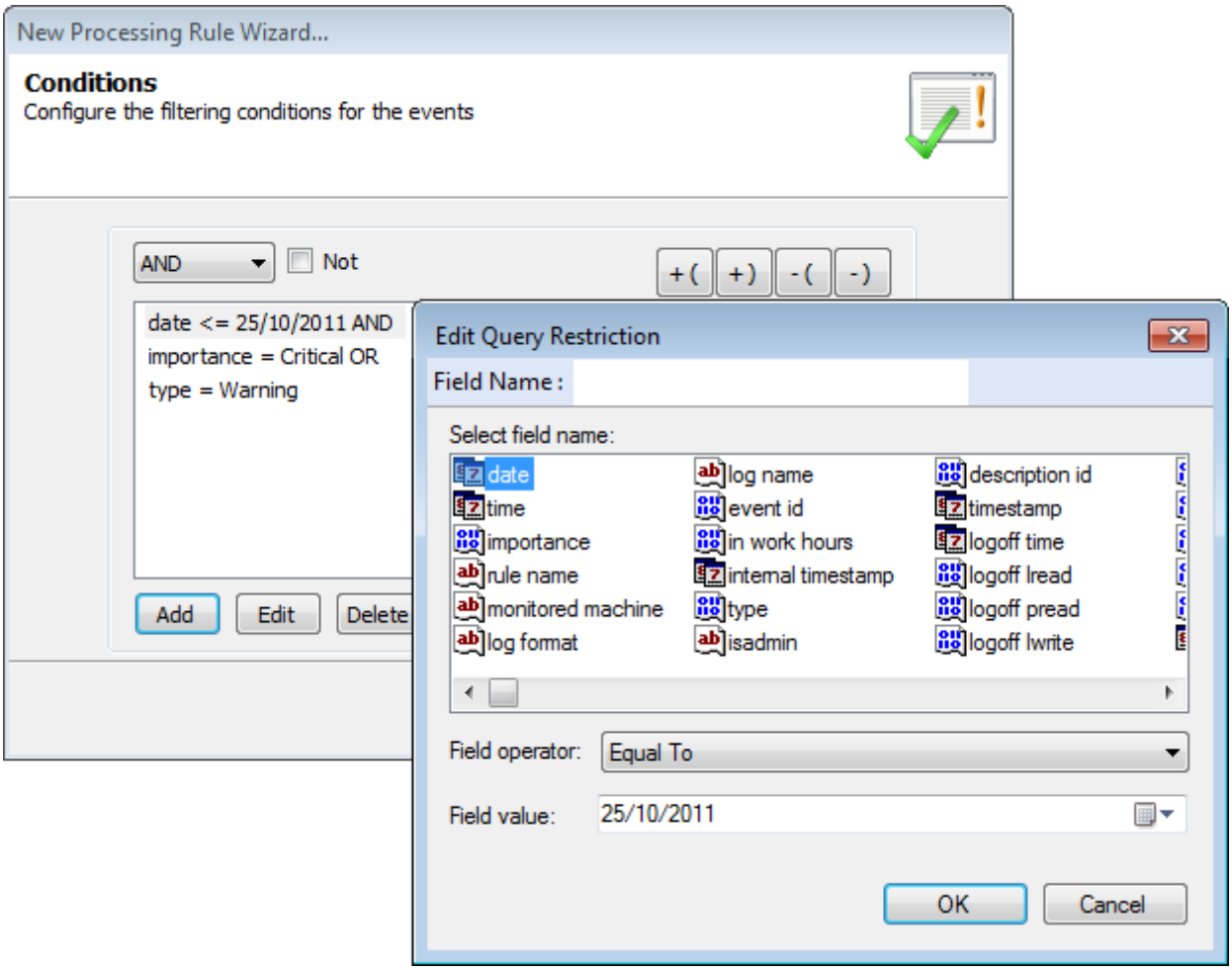
Screenshot 136: Select the logs which the rule will be applied to

4. Select the event logs to which the rule applies.

5. (Optional) Click **Add custom log...** to insert an event log which you pre-configured. Click **Next**. For more information refer to Collecting custom events.

Note

For SQL Audit, Oracle Audit, Syslogs, Text Logs and SNMP Traps messages, specify the full path of the object's log folder; example: "**C:\W3C\logs**".



Screenshot 137: Configure the rule conditions

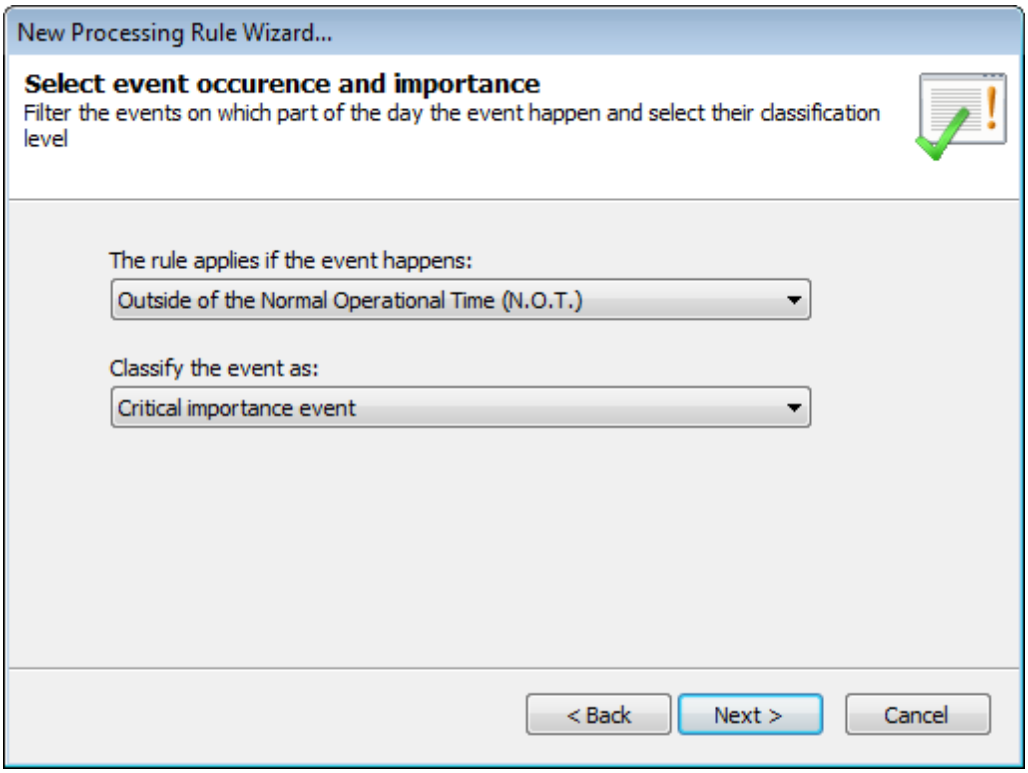
6. Click **Add** to select a field on which to base the query condition. For the selected field, specify the **Field Operator** and **Field Value**. Click **OK**.

Note

Repeat this step until all the required fields are selected. For more information refer to Building query restrictions.

Note

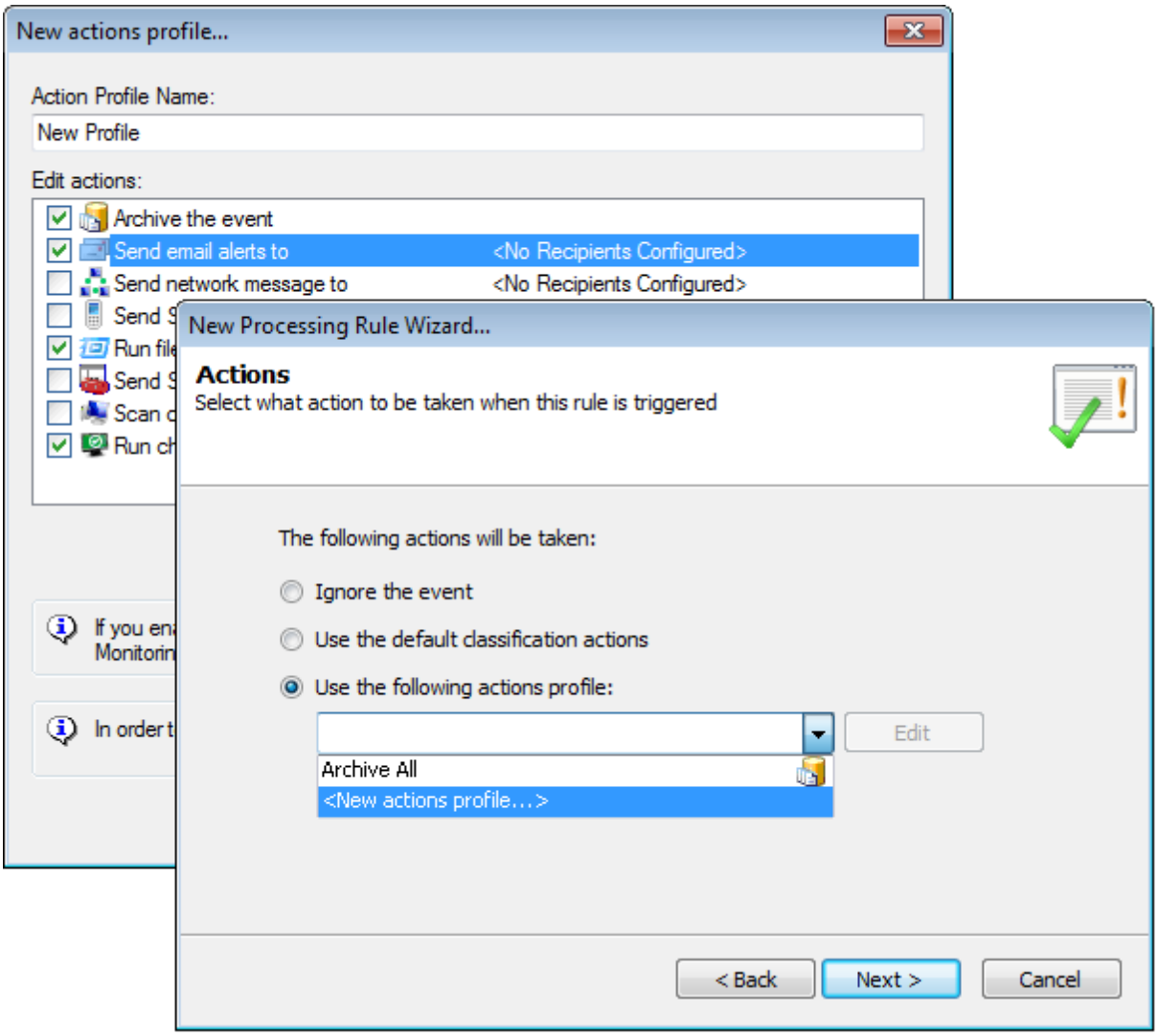
To filter events that refer to an administrator user (events having the security identifier SID that identifies a logon administrator session), ensure that if the event source is a domain member, the domain controller must also be added as an event source. For more information refer to Creating a new event source group.


New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
Outside of the Normal Operational Time (N.O.T.)
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 138: Select event occurrence and importance

7. Specify the time when the rule is applicable. Example: anytime, during working hours or outside working hours. Working and non-working hours are based on the operational time parameters configured for your event sources. For more information refer to Configuring event source operational time.

8. Select the classification (critical, high, medium, low or noise) that will be assigned to events that satisfy the conditions in this rule. Click **Next**.



Screenshot 139: Select the triggered action

9. Specify which actions are triggered by this rule and click **Next**. Available actions are:

Table 66: Configuring new events processing rules: Actions

Action	Description
Ignore the event	Select this option so that GFI EventsManager will ignore the event and not trigger any actions or notifications.
Use the default classification actions	Select this option to use the pre-configured **Default Classification Actions**.

Action	Description
Use the following actions profile	The Archive All profile is added by default. To create a new profile: 1. From the drop-down menu, select **<New actions profile...>**. This launches the **New actions profile...** dialog. 2. Specify a name for the new profile in the **Action Profile Name** text box. 3. Select the actions that you want the profile to perform. The following actions are available: » Archive the event » Send email alerts to » Send network message to » Send SMS message to » Run file » Send SNMP Message » Scan computer » Run checks on computer. **Note** If Run checks on computer is selected, ensure that the computer has monitoring checks processing enabled. For more information refer to Configuring event source monitoring. 4. For each action you select, click **Configure** to set the parameters.

10. Click **Apply** and **OK**.

Note

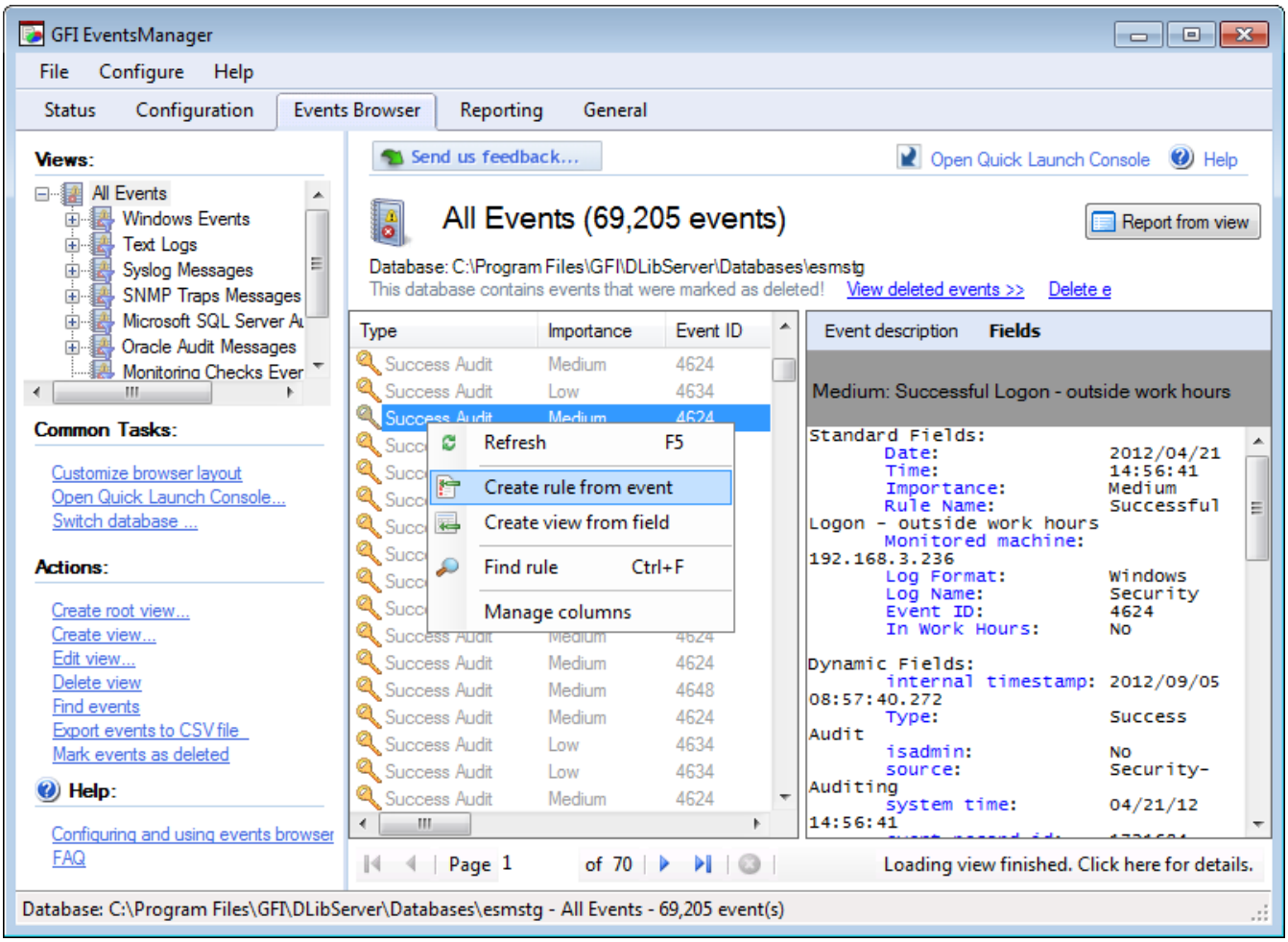
Assign the new rule(s) to your event sources. For information about how to collect event logs and process them using the specified events processing rules, refer to Collecting Event Logs.

9.4 Creating new rules from existing events

GFI EventsManager enables you to create new rules based on the information of existing events.

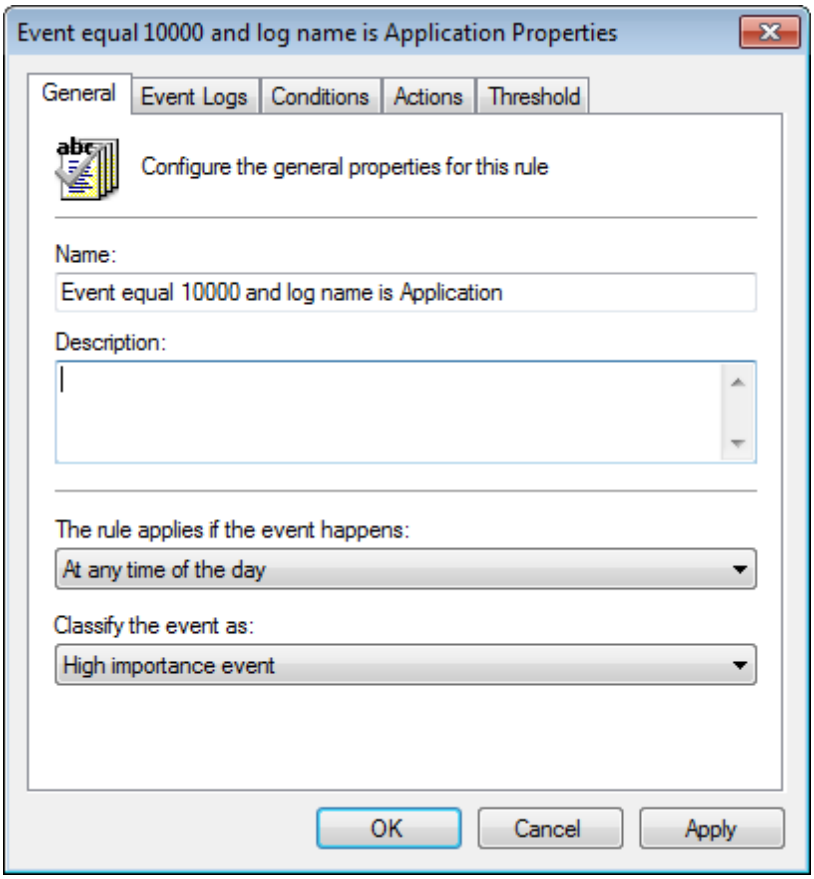
To create a new rule from an existing event:

1. From **Events Browser**, locate the event log that you want to base the rule upon.



Screenshot 140: Creating a rule from an existing event

2. Right-click the event and select **Create rule from event**.



Screenshot 141: New rule from event - General settings

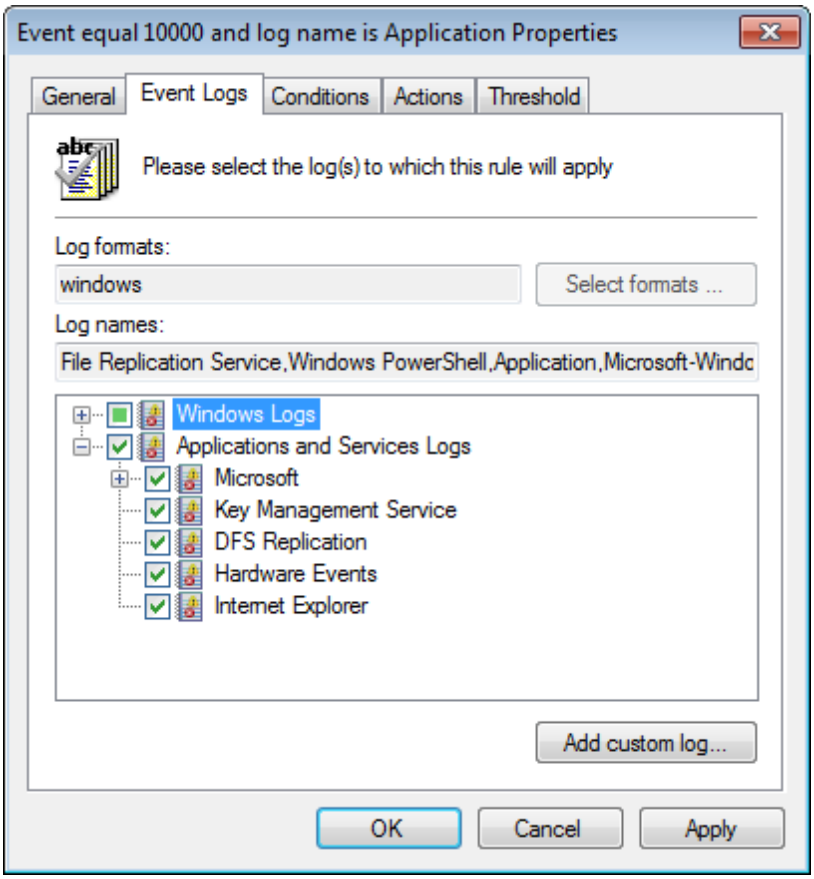
3. Specify a unique name and an optional description for the new rule.

4. From **The rule applies if the event happens** drop-down menu, select the time when the rule is applicable. Select from:

- At any time of the day
- During Normal Operational Time
- Outside the Normal Operational Time.

> **Note**
>
> For more information refer to Configuring event source operational time.

5. From the **Classify the event as** drop-down menu, select the classification level you want to assign to the event when it is generated.

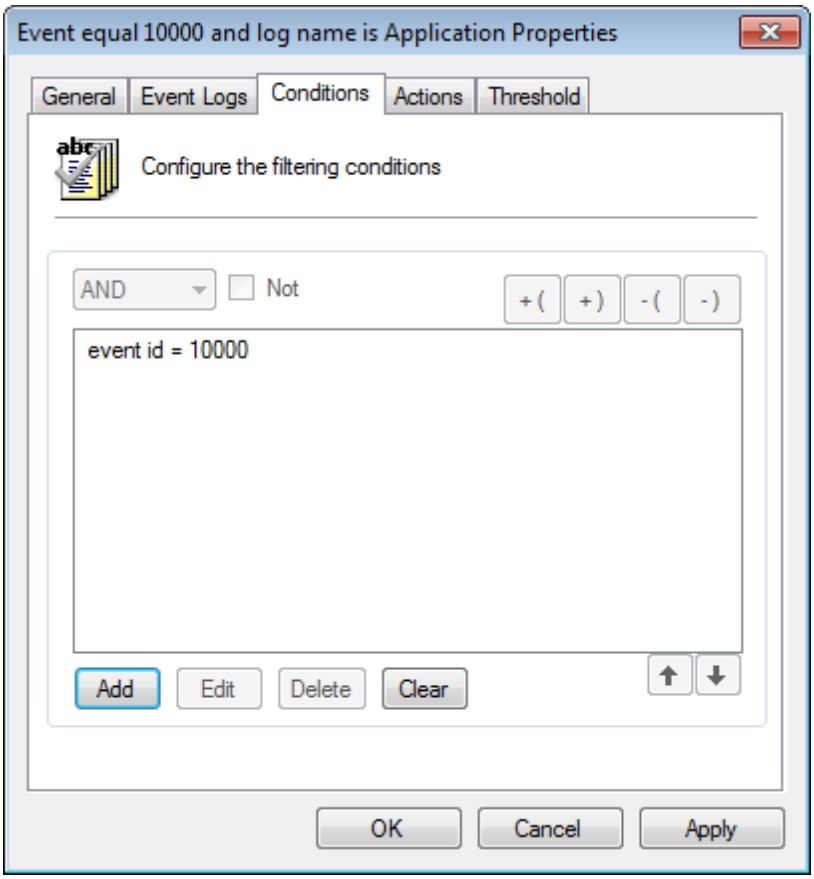


Screenshot 142: New rule from event - Select logs to collect

6. From the **Event Logs** tab, select the logs you want to collect. To add custom logs, click **Add custom log...**, specify the custom log name and click **OK**.

Note

For more information refer to Collecting custom logs.



Screenshot 143: New rule from event - Add conditions

7. Click the **Conditions** tab.Click **Add** to select a field on which to base the query condition. For the selected field, specify the **Field Operator** and **Field Value**. Click **OK**.

> **Note**
>
> Repeat this step until all the required fields are selected. For more information refer to Building query restrictions.

8. Click **Actions** tab and select what action is performed when the rule is triggered. Available options are described below:

Table 67: Available event processing rule actions

Option	Description
Ignore the event	Ignores the event until a new instance of the event is generated.
Use the default classification actions	Use the actions configured in Default Classification Actions. For more information refer to Configuring Default Classification Actions.
Use the following actions profile	From the drop-down menu, select a profile or <New action profile...> and click **Edit** to configure the action profile.

9. Click **Threshold** tab and configure the event threshold value. I.e. the number of times that an event must be detected prior to triggering alerts and remedial actions. This helps reducing false positives triggered by noise (repeated events) in your event logs.

10. Click **Apply** and **OK**.

9.5 Advanced event filtering parameters

GFI EventsManager allows systems administrators to set up advanced event filtering parameters. These options are available only for Windows® Event Logs and Syslogs. Refer to the following sections for information about:

- Windows® event filtering parameters
- Syslog filtering parameters

9.5.1 Windows® event filtering parameters

The **Event IDs:** field allows systems administrators to setup parameters described in the table below:

Table 68: Windows® event filtering parameters: Event ID field

Parameter	Description
Single events	Event IDs: 575
List of events	Event IDs: 550, 570
Range of events	Event IDs: 575-600
Combination of events	Event IDs: 550, 570, 575-600

The **Source**, **Category** and **User fields** allow systems administrators to setup parameters described in the table below:

Table 69: Windows® event filtering parameters: Source, Category and User fields

Parameter	Description
Single source name	Message: session opened
List of sources	Message: session opened, session closed
Wildcards (% and *)	Message: %session opened%

9.5.2 Syslog filtering parameters

The **Message** and **Process** fields allow systems administrators to setup parameters described in the table below:

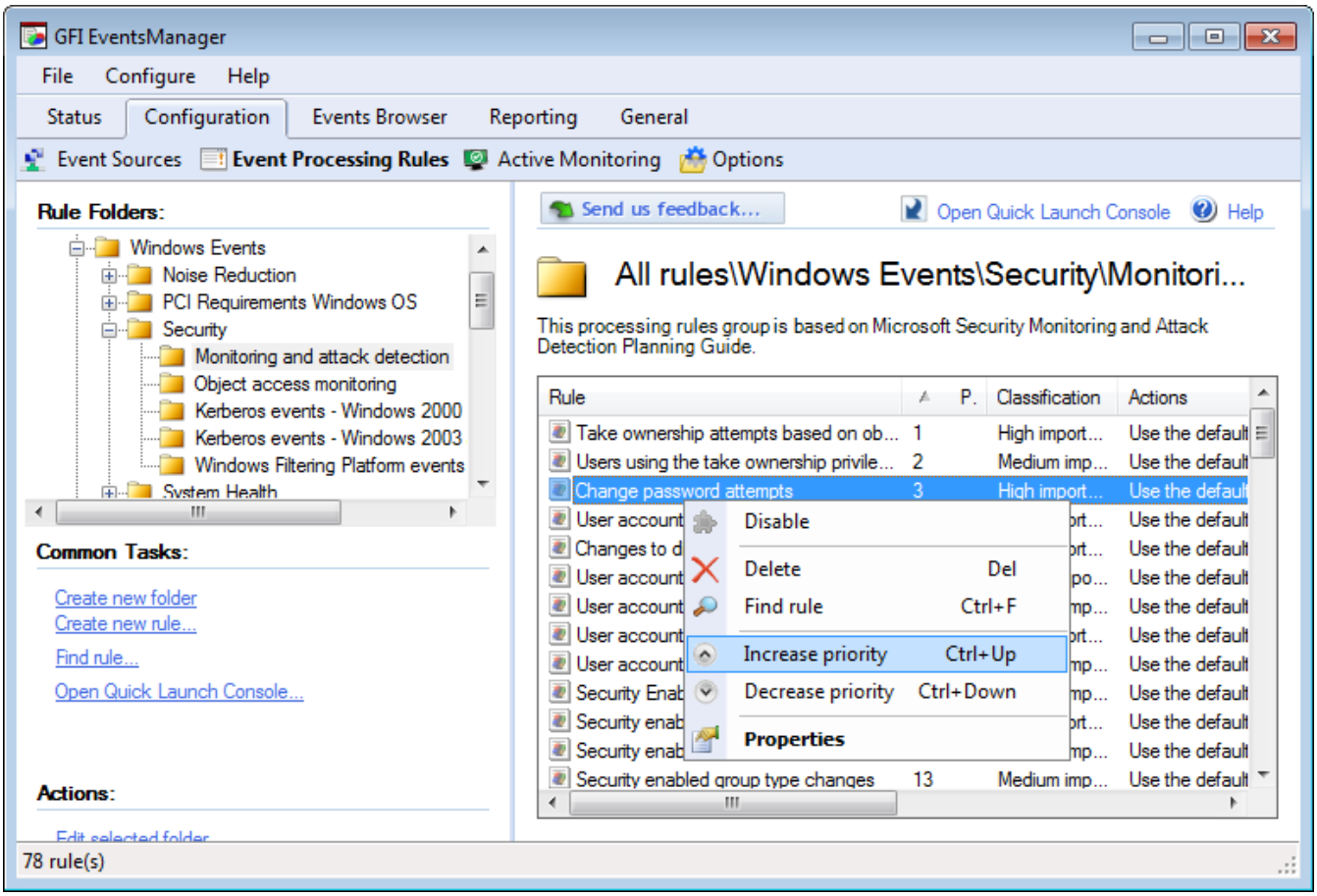
Table 70: Syslog filtering parameters: Message and Process fields

Parameters	Description
Single message	Message: session opened
List of messages	Message: session opened, session closed
Wildcards (% and *)	Message: %session opened%

9.6 Prioritizing events processing rules

Events Processing Rules are executed in order of priority. To change the order of execution:

1. From **Configuration** tab > **Events Processing Rules** > **Rule Folders**, expand a rule-set folder.



2. From the right pane, right-click a rule and select **Increase priority** or **Decrease priority** accordingly. Alternatively, select a rule and press **Ctrl+Up** to increase or **Ctrl+Down** to decrease priority.

10 Active Monitoring

Event logs are useful to track different operational aspects of devices, computers and servers, but in many cases users need more than logs to inspect this activity in further detail. To mitigate this problem, GFI EventsManager uses Active Monitoring Checks. Monitoring checks help you detect failures or irregularities automatically, so you can identify and proactively fix unexpected problems before they happen.

GFI EventsManager ships with a set of predefined checks, specifically designed to cater for Windows® operating systems, Linux/Unix operating systems, SNMP devices and Network/Internet protocols and services.

This chapter provides you with information about managing, creating and using Active Monitoring Checks.

Topics in this chapter:

10.1 About Active Monitoring Checks 190

10.2 Creating and configuring a root folder 192

10.3 Adding sub-folders to a root folder 196

10.4 Creating and configuring active monitoring checks 201

10.5 Applying active monitoring checks 206

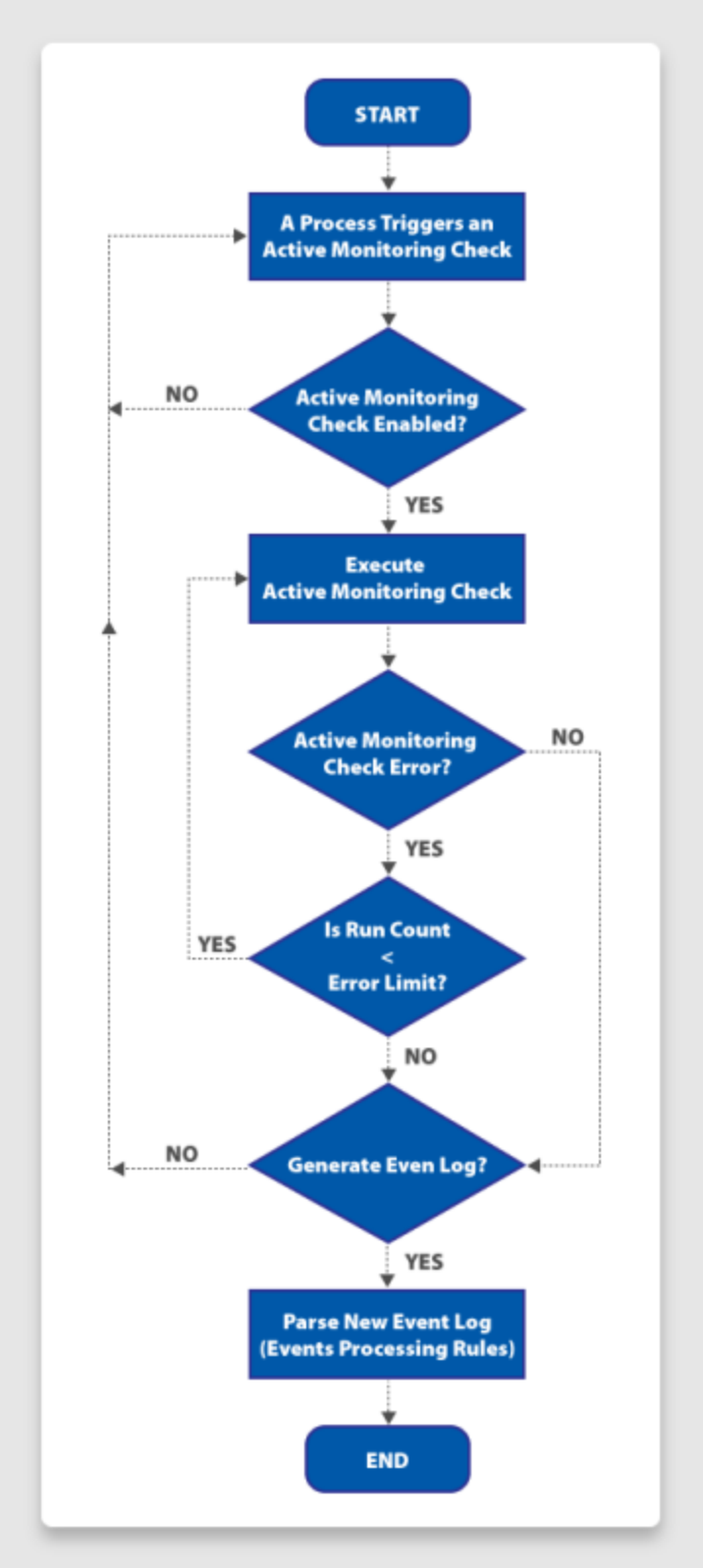
10.6 Deleting folders and monitoring checks 207

10.1 About Active Monitoring Checks

A monitoring check is a pre-configured rule, bound to a system's component or activity operation, such as CPU Usage or Ping Requests, that are used to check system availability. Active monitoring checks continuously scan event sources to determine if the configured parameter conditions are being met.

Whether a monitoring check fails or succeeds, it generates an event log from the computer that it scanned. GFI EventsManager assigns a severity rating to the generated event log.

An event processing rule can be created from the generated event log. Events processing rules can automatically trigger alerts, run additional checks and run scripts/applications to fix the problem that generated the log.



Screenshot 144: How Active Monitoring Checks work

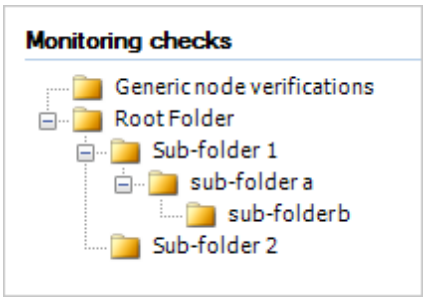
Example

You configure a monitoring check to generate an event log when a computer's free hard disk spaces reaches a pre-configured limit. To achieve this:

1. When the limit is reached and the monitoring check generates an event, locate it in Events Browser and create an event processing rule based on it. For more information refer to Creating new rules from existing events.

2. Configure the new events processing rule conditions to ignore non-matching events. For more information refer to Creating new events processing rules.

3. Configure the new rule to trigger an alert or action, to resolve the problem. For more information refer to Configuring Default Classification Actions.



Screenshot 145: Root folder and sub-folder structure

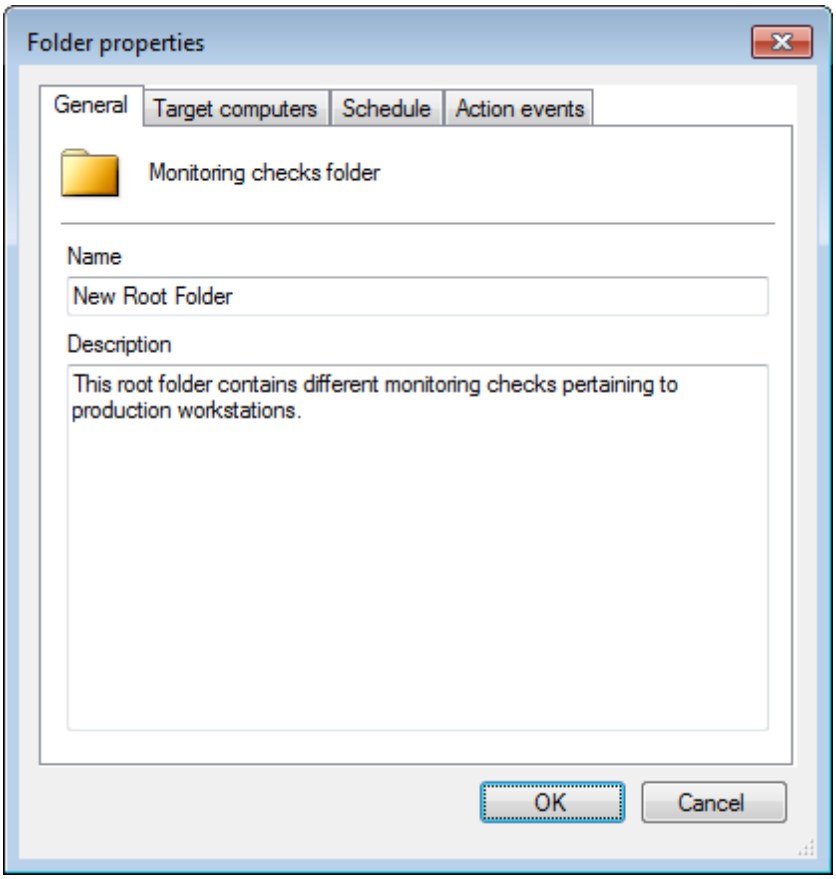
Checks are organized in Root Folders and Sub-Folders. Objects inherit settings from their parent folder. This enables you to configure a number of monitoring checks simultaneously.

10.2 Creating and configuring a root folder

A root folder is a parent folder that can contain a set of sub-folders and Active Monitoring. Every child object of a root folder inherits the same settings. This enables swift configuration of multiple monitoring checks and sub-folder.

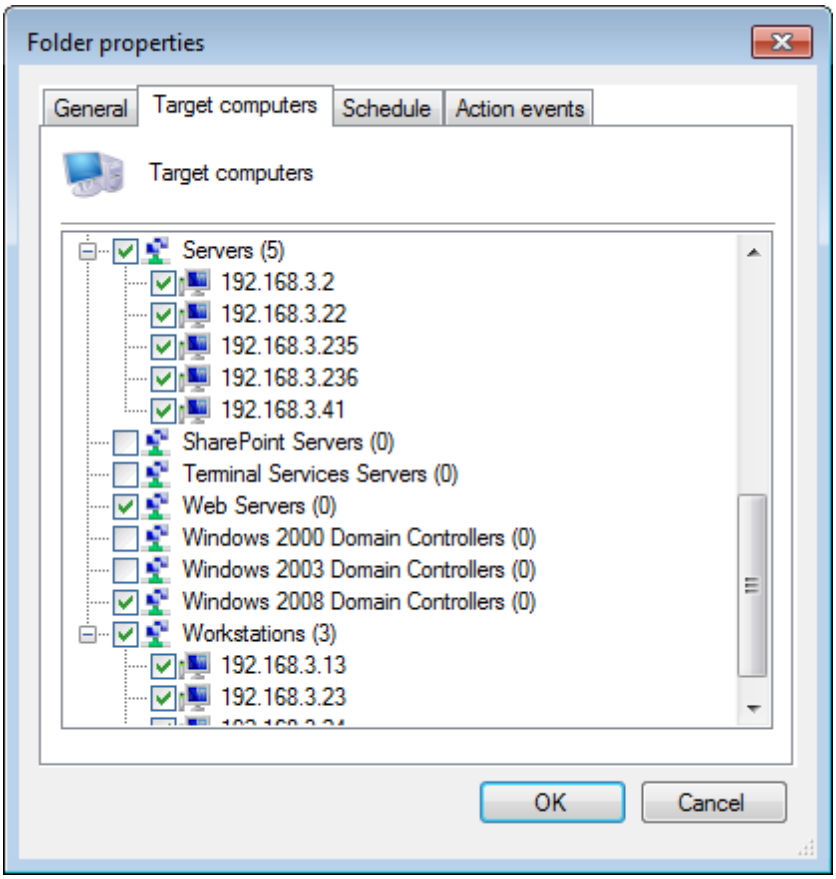
To create a new root folder:

1. From **Configuration** tab **> Active Monitoring > Common Tasks**, click **Create root folder**. This opens the **Folder properties** dialog.



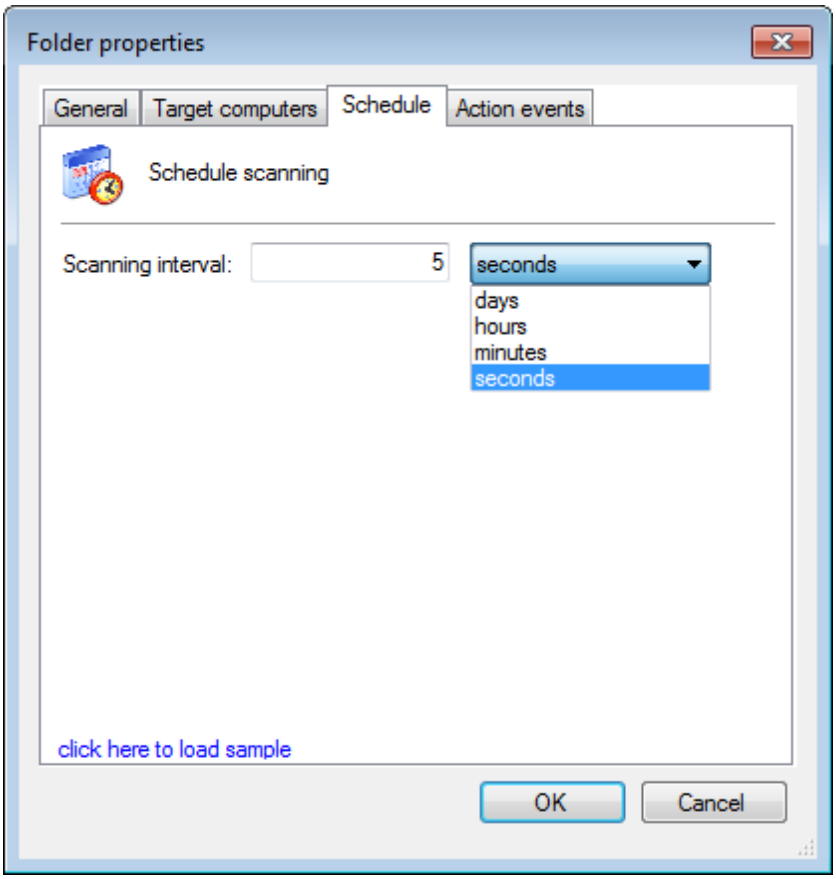
Screenshot 146: Folder properties - General tab

2. Specify a unique name and an optional description in the **Name** and **Description** fields.



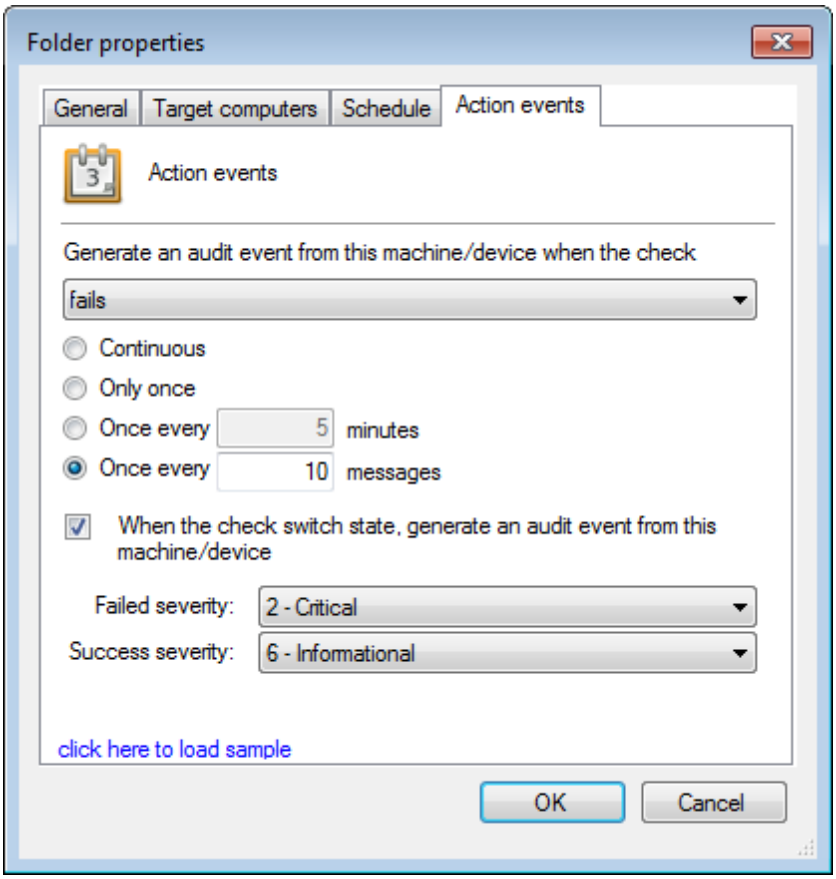
Screenshot 147: Folder properties - Target computer tab

3. Click **Target computers** tab and select the event sources. Active Monitoring added to this new folder are applied to the selected event sources.



Screenshot 148: Folder properties - Schedule tab

4. From the **Schedule** tab, set the time interval when GFI EventsManager runs the monitoring check (s) on the selected event sources. By default, a monitoring check interval is set to 5 seconds.



Screenshot 149: Folder properties - Action events tab

Note

Regardless of whether Active Monitoring fails or succeeds, the computer that it checks generates an event log. This event log can be processed by events processing rules which can trigger alerts or run scripts/applications for remedial operations. For more information refer to Creating new rules from existing events.

5. From the **Action events** tab, configure when event logs are generated and how GFI EventsManager classifies the generated events.
Available options are described in the following table:

Table 71: Monitoring checks - Action events

Option	Description
Generate an audit event from this machine/device when the check	GFI EventsManager enables you to generate event logs after the event source is checked for irregularities. From the drop-down menu, select: » **Fails** - generate an event log when the conditions of the check fails » **Succeeds** - generate an event log when the conditions of the check succeeds » **Fails or Succeeds** - generates an event log every time the check is run on the specified event source(s).
Continuous	Generates an event log every time the check fails/succeeds/both.
Only once	Generates an event log the first time the check fails/succeeds/both.
Once every {X} minutes	Generates an event log once every number of minutes you specify.

Option	Description
Once every {X} messages	Generates an event log once every number of messages you specify. Example: if you key in 10, only one event log is generated for every 10 times the check fails/succeeds/both.
When the check switch state, generate an audit event from this machine/device	Generate an event log when the check changes state from Fail to Succeed or vice versa.
Failed severity	Select the severity rating that GFI EventsManager assigns to the event log of a failed system check.
Success severity	Select the severity rating that GFI EventsManager assigns to the event log of a successful system check.

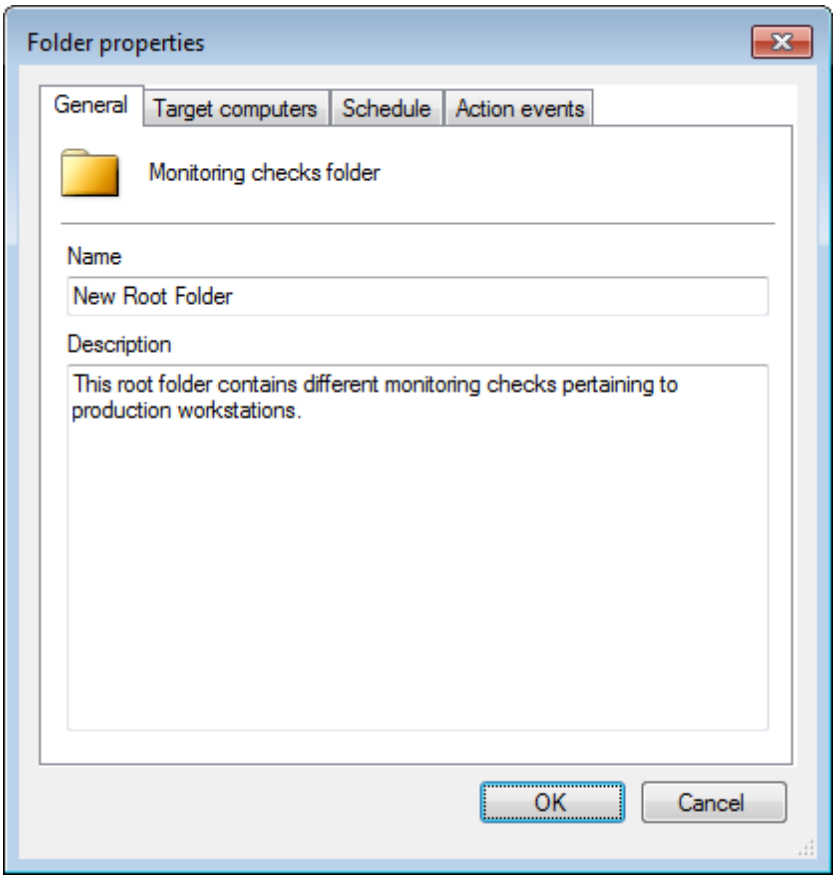
6. Click **OK**.

10.3 Adding sub-folders to a root folder

Sub-folders are used to sub-divide a group of monitoring checks that share some common properties, but may (for example) be targeted towards different types of event sources.

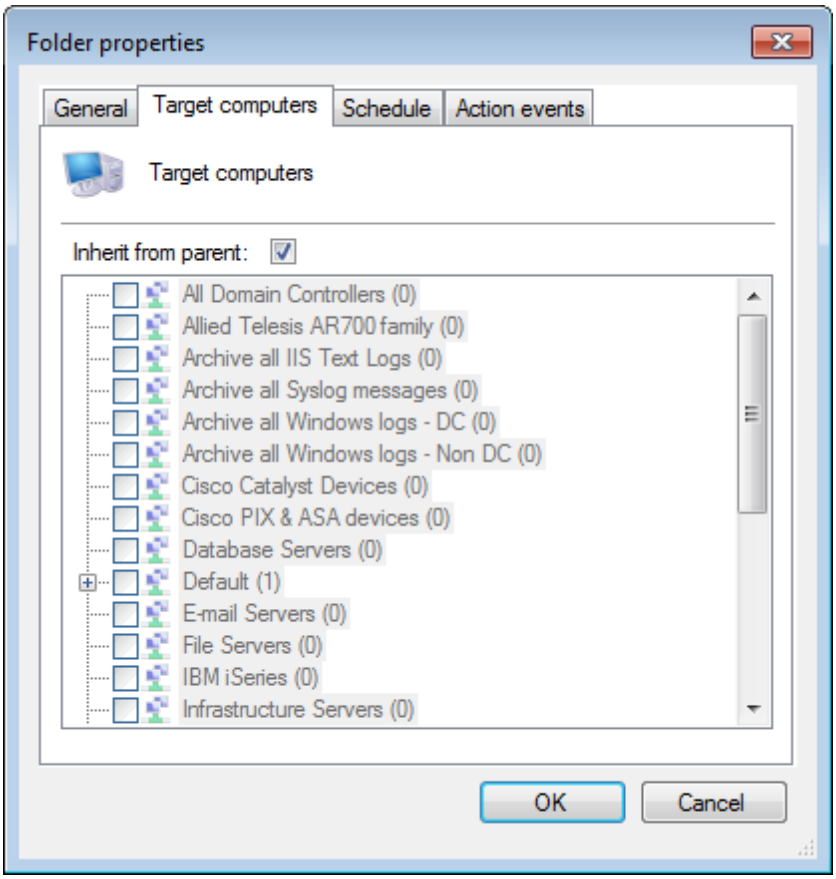
To add a new sub-folder:

1. From **Configuration > Active Monitoring > Monitoring checks**, right-click a root folder/sub-folder and select **Create new folder**.



Screenshot 150: Folder properties - General tab

2. From the **General** tab, key in a name for the new folder and an optional description.

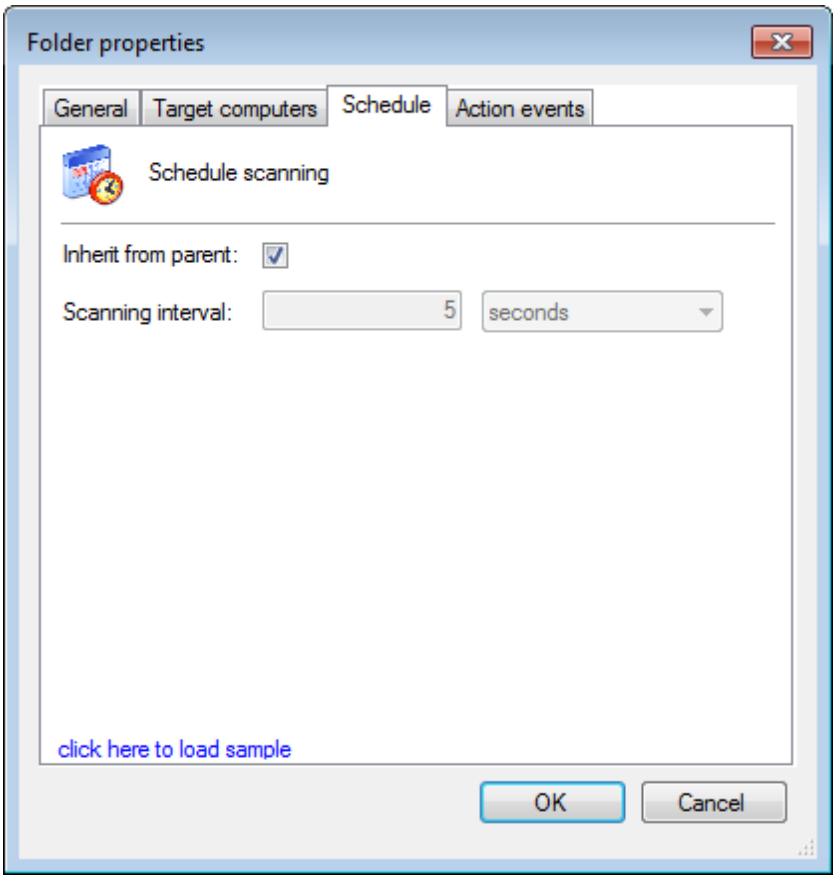


Screenshot 151: Folder properties - Target computer tab

Note

Select **Inherit from parent** to use the same settings as the parent folder.

3. Click the **Target computers** tab and select the event sources. Active Monitoring that are added to this new folder are applied to the selected event sources.

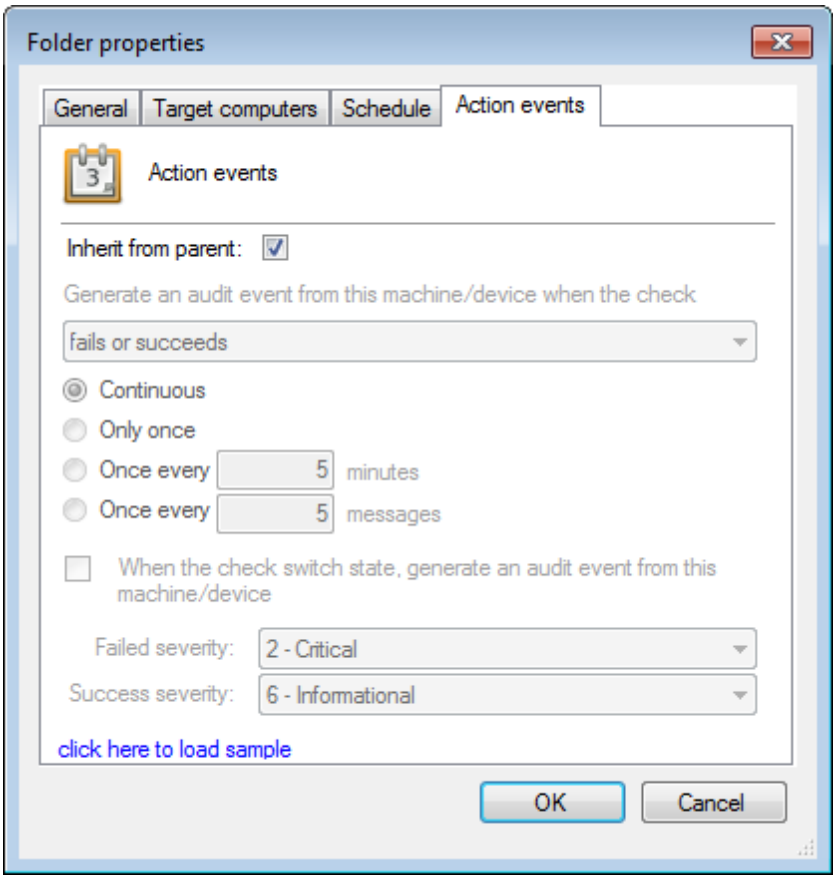


Screenshot 152: Folder properties - Schedule tab

Note

Select **Inherit from parent** to use the same settings as the parent folder.

4. From the **Schedule** tab, set the interval when GFI EventsManager runs the monitoring check(s) on the selected event sources. By default, a monitoring check interval is set to 5 seconds.



Screenshot 153: Folder properties - Action events tab

Note

Regardless of whether Active Monitoring fails or succeeds, the computer that it checks generates an event log. This event log can be processed by events processing rules which can trigger alerts or run scripts/applications for remedial operations. For more information refer to Creating new rules from existing events.

Note

Select **Inherit from parent** to use the same settings as the parent folder.

5. From the **Action events** tab, configure when event logs are generated and how GFI EventsManager classifies the generated events.
Available options are described in the following table:

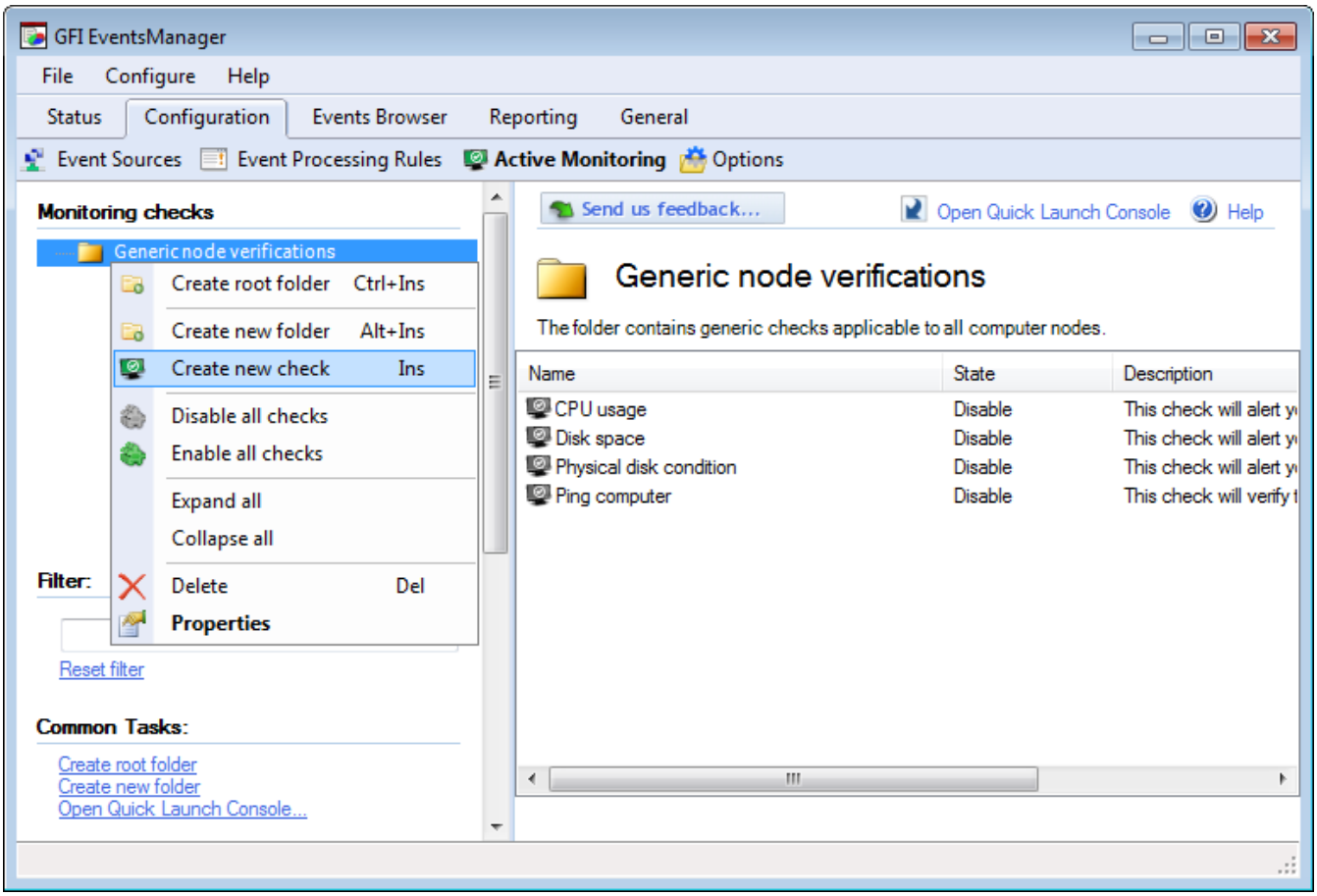
Table 72: Monitoring checks - Action events

Option	Description
Generate an audit event from this machine/device when the check	GFI EventsManager enables you to generate event logs after the event source is checked for irregularities. From the drop-down menu, select: » **Fails** - generate an event log when the conditions of the check fails » **Succeeds** - generate an event log when the conditions of the check succeeds » **Fails or Succeeds** - generates an event log every time the check is run on the specified event source(s).
Continuous	Generates an event log every time the check fails/succeeds/both.
Only once	Generates an event log the first time the check fails/succeeds/both.
Once every {X} minutes	Generates an event log once every number of minutes you specify.
Once every {X} messages	Generates an event log once every number of messages you specify. Example: if you key in 10, only one event log is generated for every 10 times the check fails/succeeds/both.
When the check switch state, generate an audit event from this machine/device	Generate an event log when the check changes state from Fail to Succeed or vice versa.
Failed severity	Select the severity rating that GFI EventsManager assigns to the event log of a failed system check.
Success severity	Select the severity rating that GFI EventsManager assigns to the event log of a successful system check.

6. Click **OK**.

10.4 Creating and configuring active monitoring checks

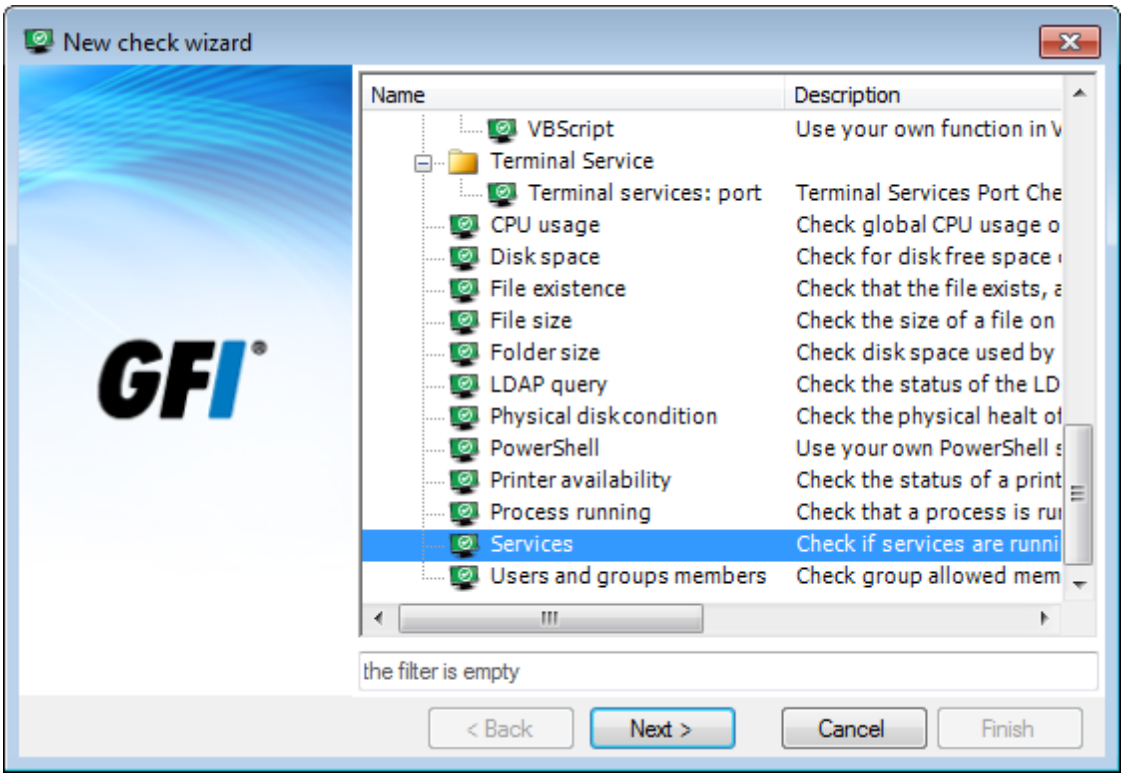
To create a new active monitoring check:



Screenshot 154: Creating a new active monitoring check

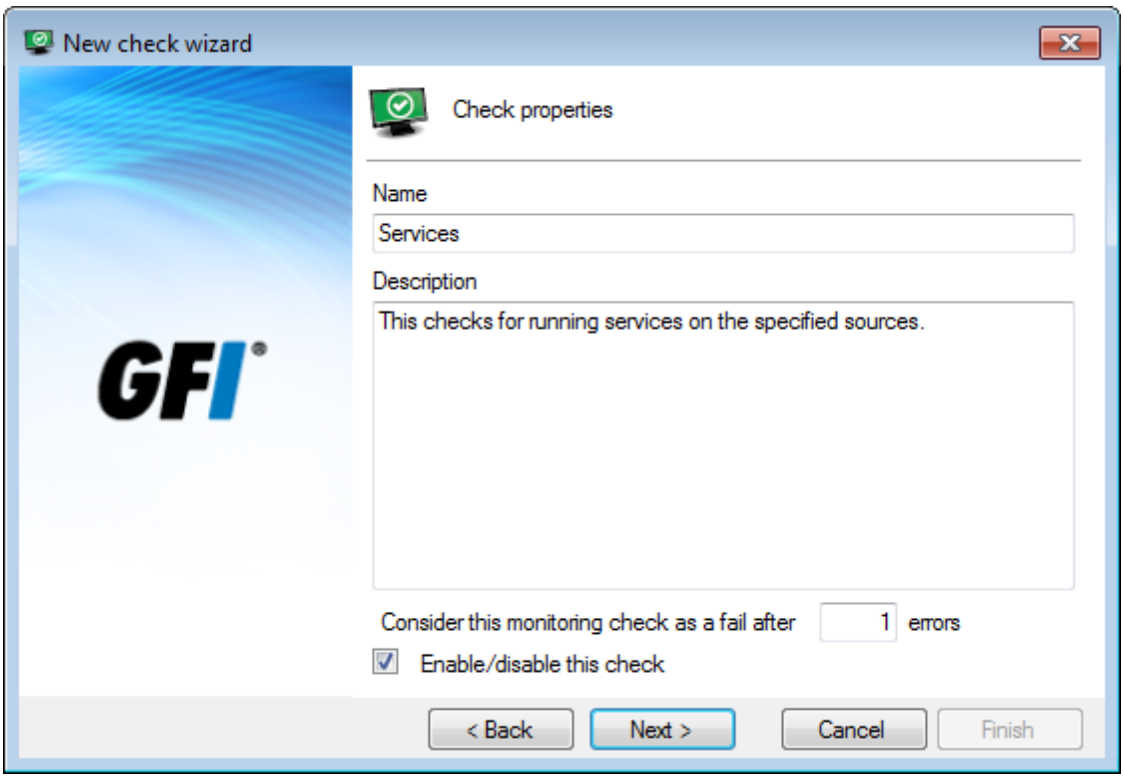
1. Click **Configuration > Active Monitoring**.

2. Right-click the root/sub-folder where you want the new monitoring check to be saved and select **Create new check**.



Screenshot 155: Select check type

3. Select the check type and click **Next**.

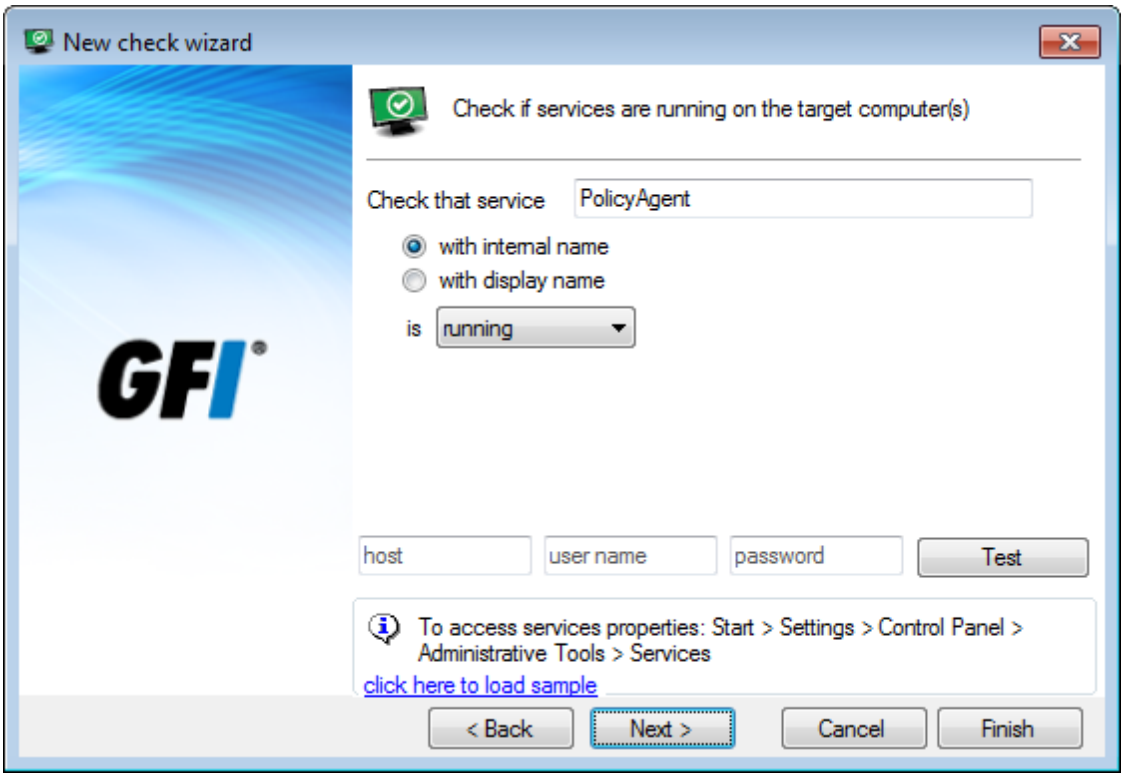


Screenshot 156: Configure general check properties

4. Specify a unique name and an optional description in the **Name** and **Description** fields.

5. In **Consider this monitoring check as fail after {X} errors** text box specify the number of errors that must occur, before the new checks is classified as **Failed**.

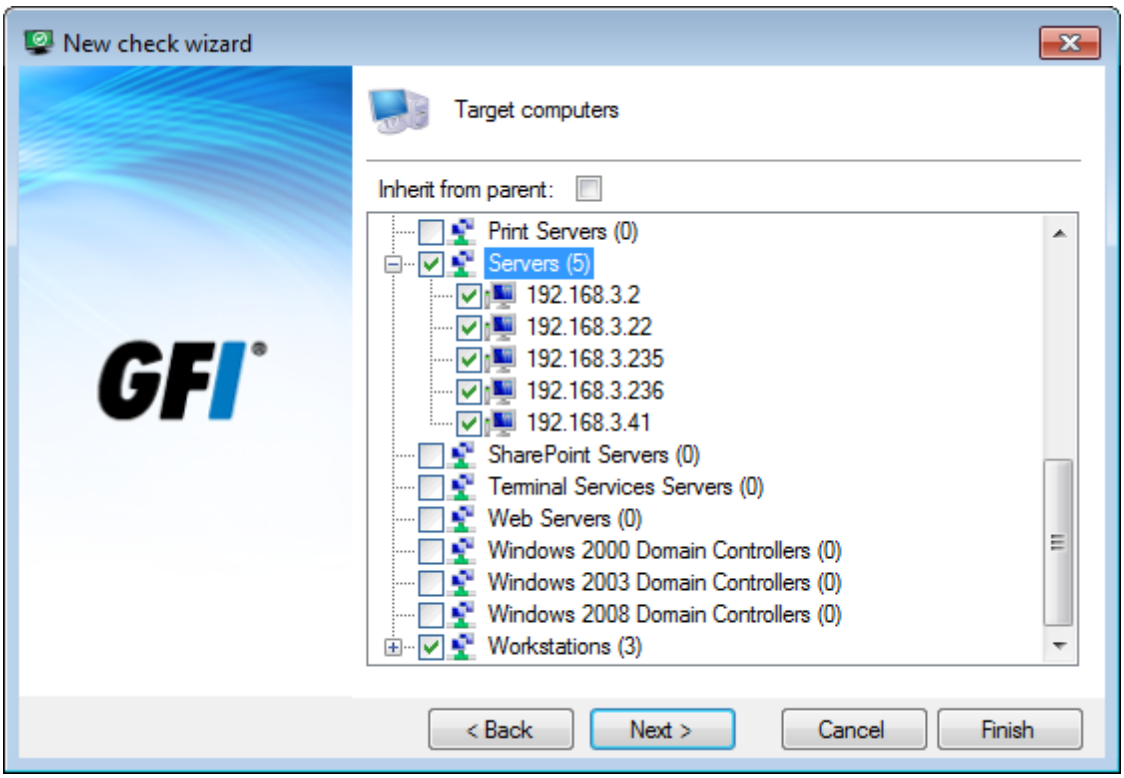
6. Select/unselect **Enable/disable this check**, to turn on/off the new monitoring check. Click **Next**.



Screenshot 157: Configure monitoring check parameters

7. Configure the parameters that have to be checked and click **Next**.

> **Note**
>
> This step is different for each different type of check you select in step 3.

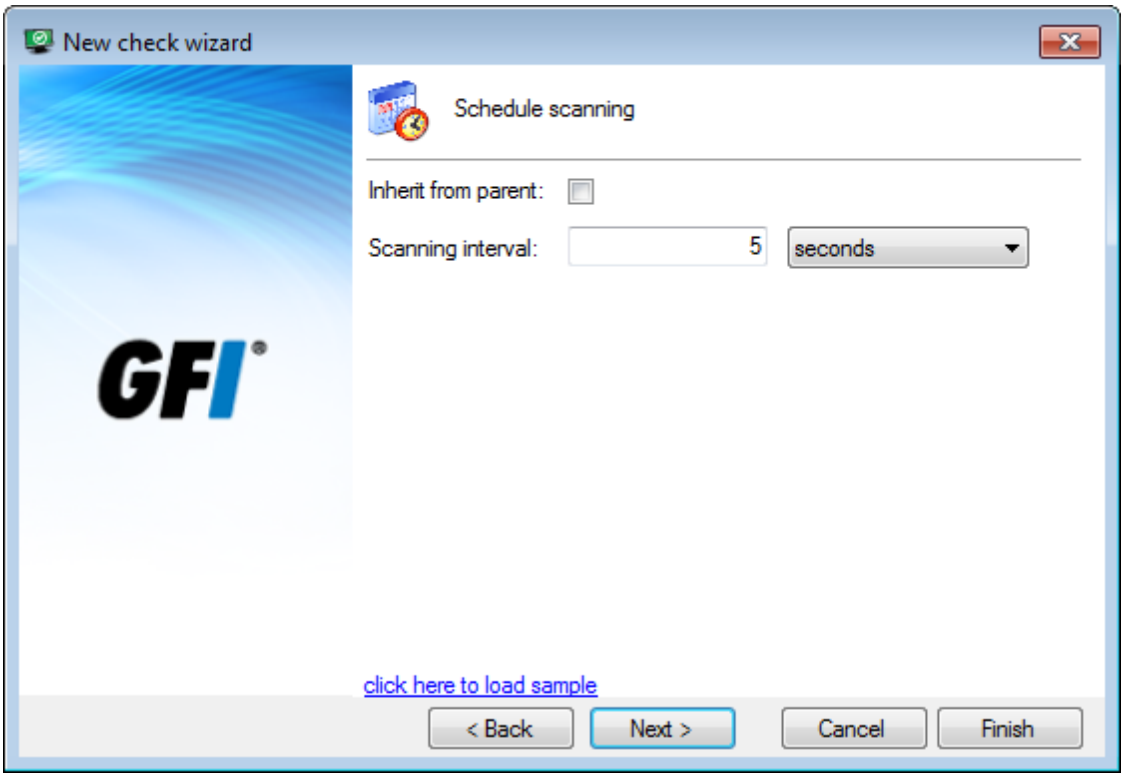


Screenshot 158: Select the effected sources

Note

Select **Inherit from parent** to use the same settings as the parent folder.

8. From the list of event sources, select the computers to monitor by this new check. Click **Next**.

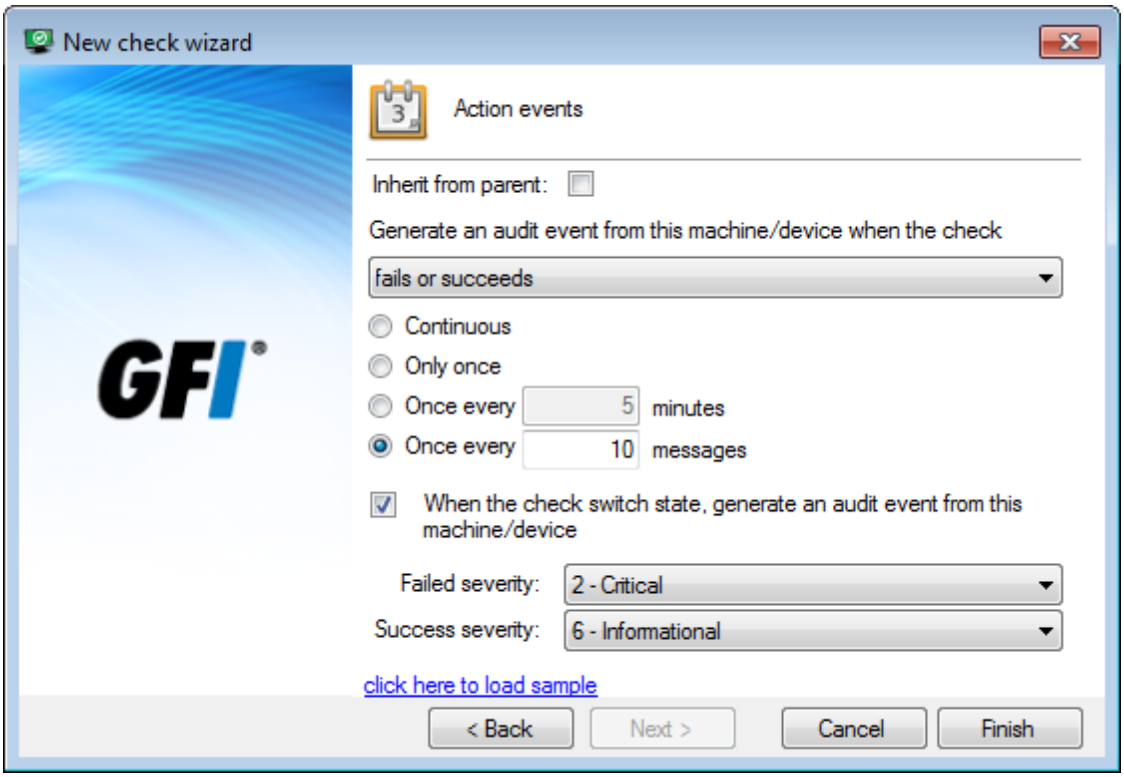


Screenshot 159: Set the scan time interval

Note

Select **Inherit from parent** to use the same settings as the parent folder.

9. Configure the scan interval schedule for the new check. By default, the check scans the selected source(s) once every 5 seconds.


New check wizard
Action events
Inherit from parent:
Generate an audit event from this machine/device when the check
fails or succeeds
Continuous
Only once
Once every 5 minutes
Once every 10 messages
When the check switch state, generate an audit event from this machine/device
Failed severity: 2 - Critical
Success severity: 6 - Informational
click here to load sample
< Back
Next >
Cancel
Finish

Screenshot 160: Configure event log actions

Note

Select **Inherit from parent** to use the same settings as the parent folder.

10. A monitoring check generates an event log regardless of whether it fails or succeeds. From **Action events**, when event logs are generated and how GFI EventsManager classifies the generated logs. Available options are described in the following table:

Table 73: Monitoring checks - Action events

Option	Description
Generate an audit event from this machine/device when the check	GFI EventsManager enables you to generate event logs after the event source is checked for irregularities. From the drop-down menu, select: » **Fails** - generate an event log when the conditions of the check fails » **Succeeds** - generate an event log when the conditions of the check succeeds » **Fails or Succeeds** - generates an event log every time the check is run on the specified event source(s).
Continuous	Generates an event log every time the check fails/succeeds/both.
Only once	Generates an event log the first time the check fails/succeeds/both.
Once every {X} minutes	Generates an event log once every number of minutes you specify.
Once every {X} messages	Generates an event log once every number of messages you specify. Example: if you key in 10, only one event log is generated for every 10 times the check fails/succeeds/both.
When the check switch state, generate an audit event from this machine/device	Generate an event log when the check changes state from Fail to Succeed or vice versa.
Failed severity	Select the severity rating that GFI EventsManager assigns to the event log of a failed system check.

Option	Description
Success severity	Select the severity rating that GFI EventsManager assigns to the event log of a successful system check.

11. Click **Finish**.

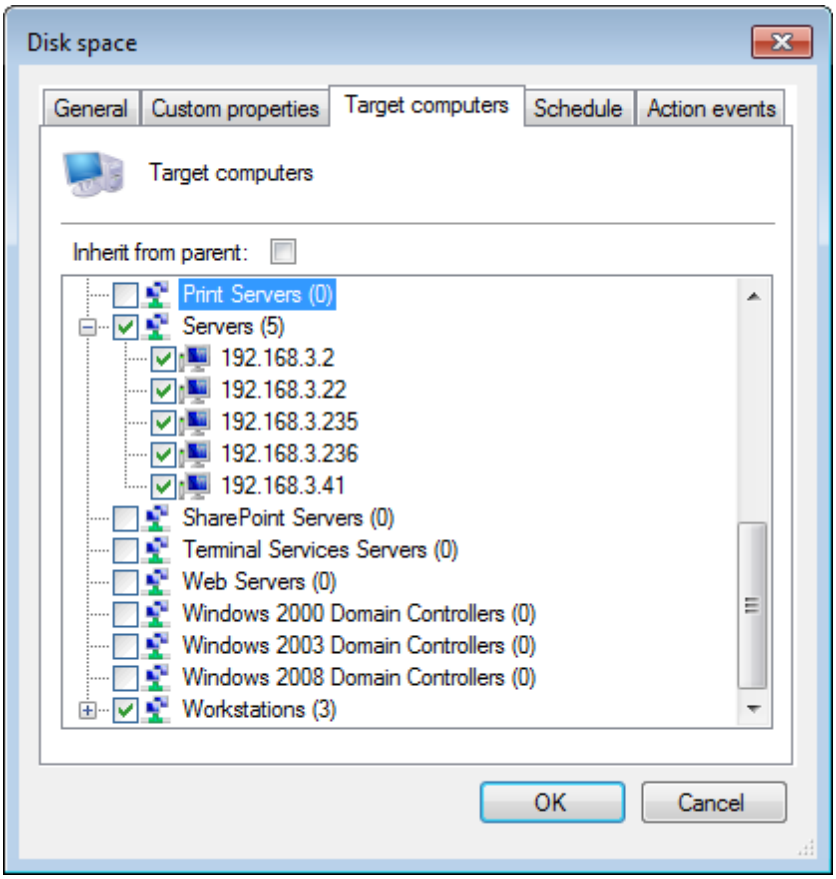
10.5 Applying active monitoring checks

Active Monitoring can be applied to single event sources or groups of event sources. Event sources can be selected on a check-by-check basis or at root folder level. Configuring settings at folder level enables the pertaining checks to inherit the same event source settings.

To assign a pre-configured monitoring check:

1. Go to **Configuration > Active Monitoring**.

2. Right-click on the monitoring check/folder that you want to assign to your event sources and select **Properties**.



Screenshot 161: Target computers tab

3. From the **Target computers** tab, select the event source or group of event sources.

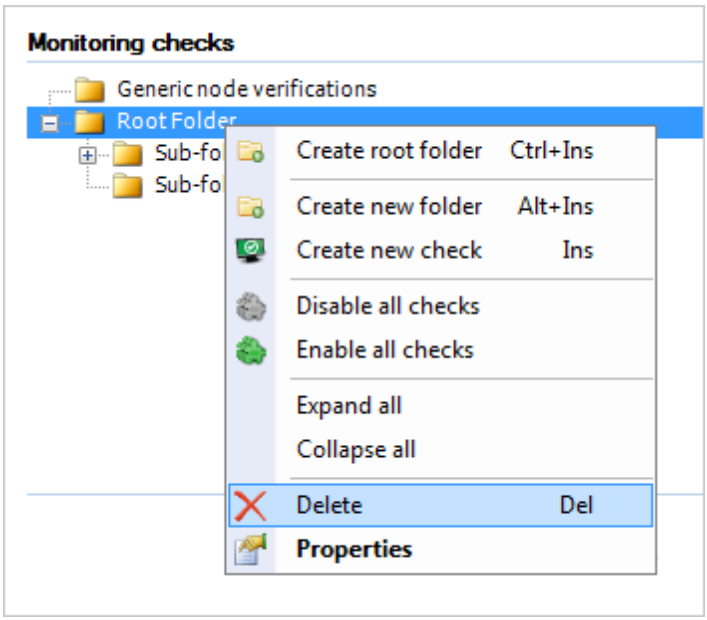
4. Click **OK**.

> **Note**
>
> Select **Inherit from parent** to use the same settings as the parent folder.

10.6 Deleting folders and monitoring checks

To delete a folder/monitoring check:

1. Go to **Configuration > Active Monitoring**.



Screenshot 162: Deleting folders and monitoring checks

2. From the **Monitoring checks** section, right-click the folder/monitoring check to delete and select **Delete**.

Important

Deleting a root folder (parent folder), deletes all the contents as well. Make sure that you delete unwanted items only.

11 Alerts and Default Actions

This chapter provides you with information about the available alerting methods and how to configure each according to your requirements. During event processing, GFI EventsManager automatically executes actions and triggers alerts whenever particular events are encountered.

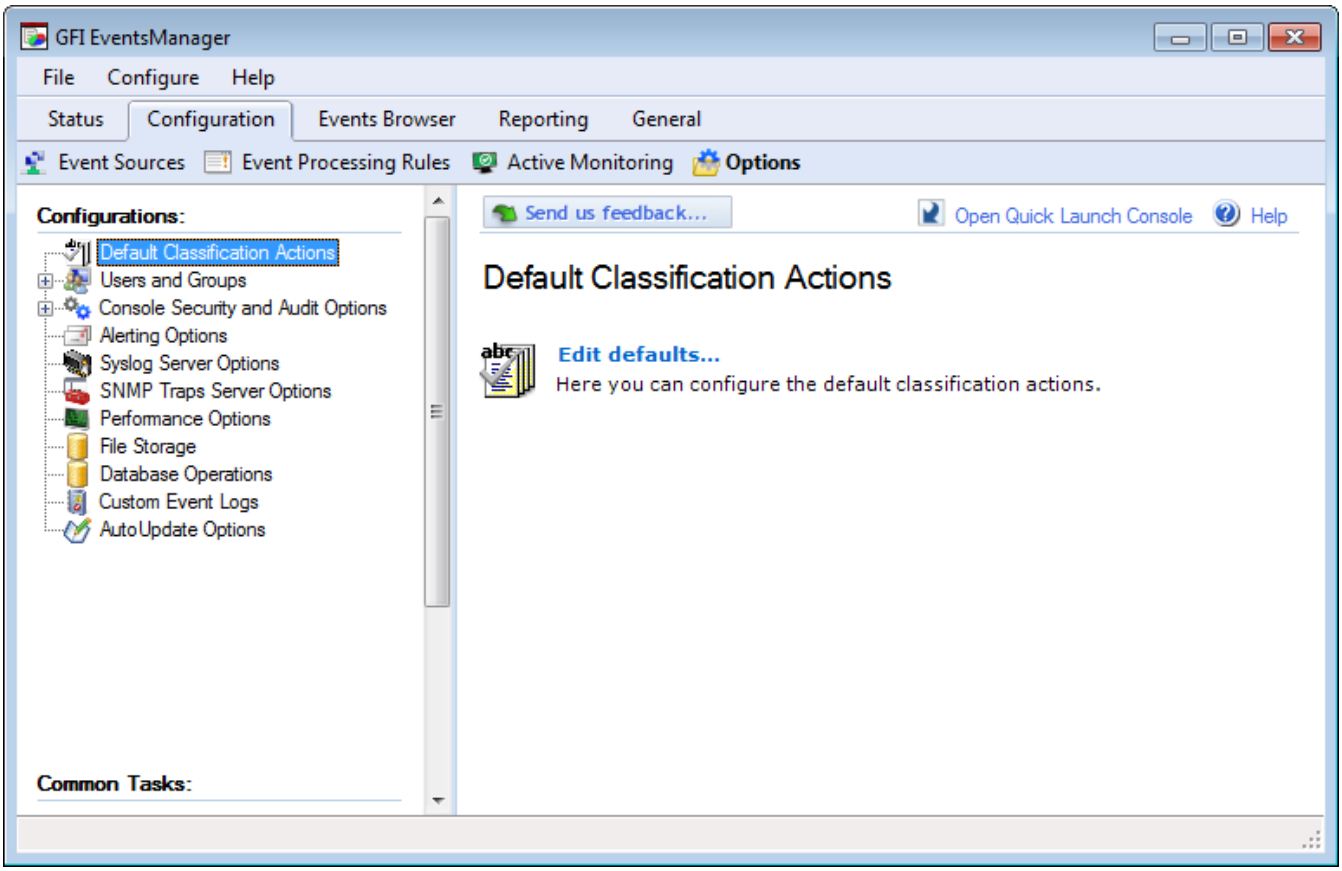
Topics in this chapter:

11.1 Configuring Default Classification Actions 208

11.2 Configuring Alerting Options 210

11.1 Configuring Default Classification Actions

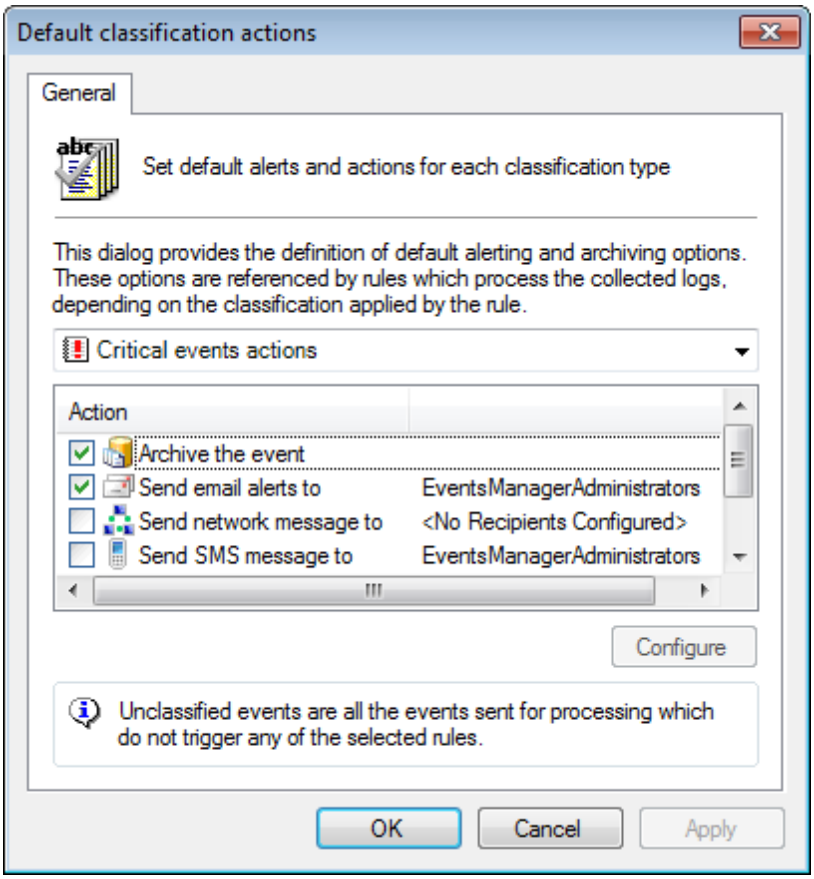
Through the configuration parameters provided in the default classification actions, you can trigger alerts and actions based only on event classification. Example: default classification parameters can be configured to trigger email alerts for all classified events (critical, high, medium and low) but archive only critical events.



Screenshot 163: Configuring default classification actions

To configure Default Classification Actions:

1. From **Configuration** tab > **Options**, right-click **Default Classification Actions** node and **Edit defaults…**


Default classification actions
General
Set default alerts and actions for each classification type
This dialog provides the definition of default alerting and archiving options. These options are referenced by rules which process the collected logs, depending on the classification applied by the rule.
Critical events actions
Action
Archive the event
Send email alerts to
EventsManagerAdministrators
Send network message to
<No Recipients Configured>
Send SMS message to
EventsManagerAdministrators
Configure
Unclassified events are all the events sent for processing which do not trigger any of the selected rules.
OK
Cancel
Apply

Screenshot 164: Default Classification Actions dialog

2. From the drop-down menu, select the event classification to be configured.

3. From **Action** list, select actions to be triggered and click **Configure**. The available actions are:

Table 74: Default Classification Actions

Action	Description
Archive the event	Archives events without further processing.
Send email alerts to	Click **Configure** and select the recipients. **NOTE** Ensure that users have a valid email address configured. For more information refer to Managing user accounts.
Send network messages to	Click **Configure** and select the recipients. **NOTE** Ensure that users have a valid computer name/IP configured. For more information refer to Managing user accounts.
Send SMS message to	Click **Configure** and select the recipients. **NOTE** Ensure that users have a valid mobile number configured. For more information refer to Managing user accounts.

Action	Description
Run file	Click **Configure** and select the file to execute and specify any command-line parameters you want to pass to the file. Supported files include: » VB Scripts - *.VBS » Batch Files - *.BAT » Executables - *.EXE
Send SNMP Message	Click **Configure** and select the recipients.
Scan computer	GFI EventsManager re-audits the computer.
Run checks on computer	Click **Configure**, select the monitoring checks you want to run when the action is triggered. **Note** Active Monitoring is applied to the corresponding event sources, selected from the Target computers tab. For more information refer to Creating and configuring Active Monitoring checks. **Note** Ensure that Monitoring Checks processing is enabled or the checks will be discarded. For more information refer to Configuring event source monitoring.

4. Click **Apply** and **OK**.

Note

Running default actions on events classified as **Low**, may cause a lot of network traffic when email, SMS, network or SNMP alerts are enabled. This may also be problematic when archiving is enabled on Low importance events.

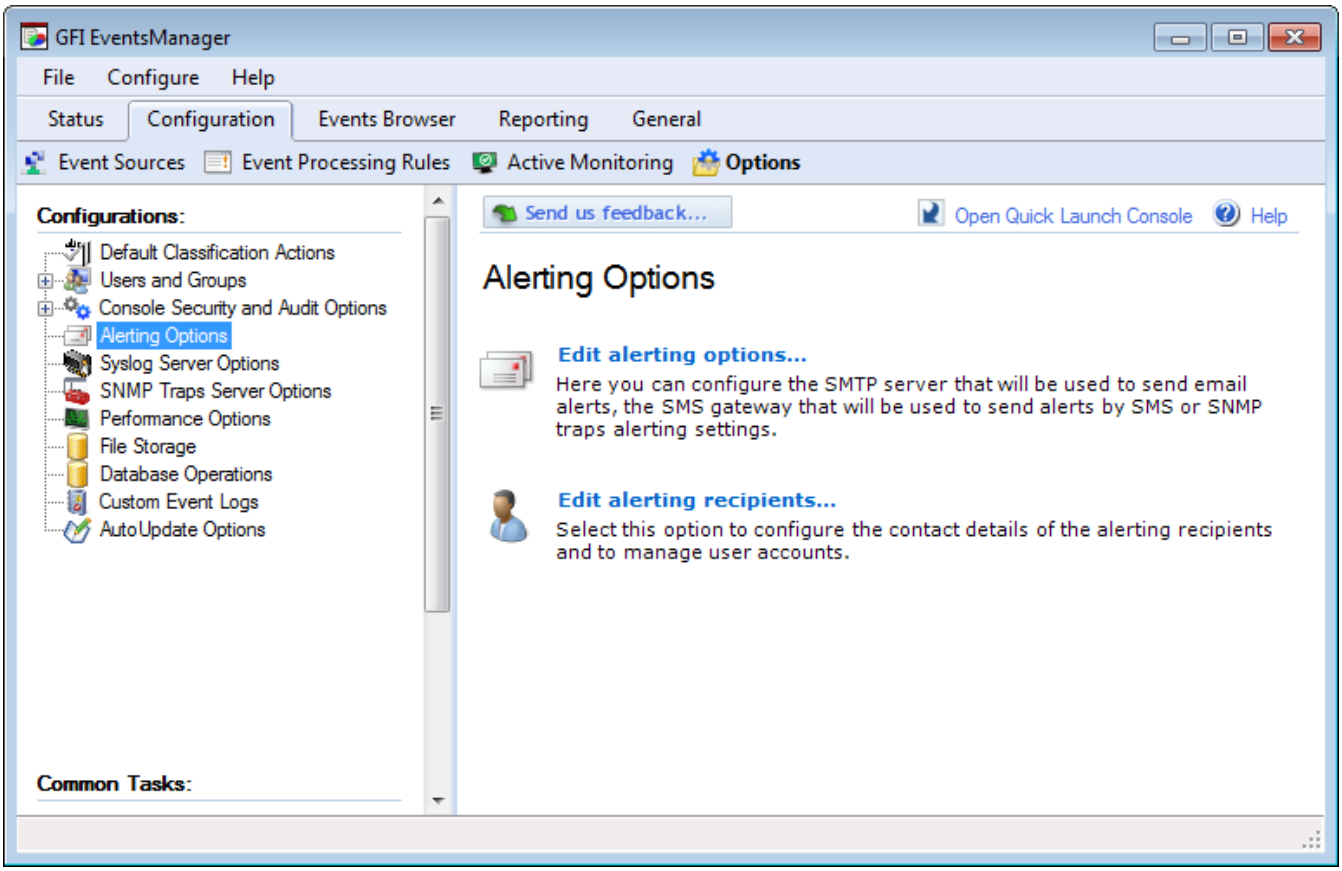
11.2 Configuring Alerting Options

Alerting options enable you to configure what alerts are triggered when particular event(s) are encountered. For example, you can configure GFI EventsManager to send an email and SMS alert to one or more recipients when a **Critical** event is processed.

This section contains information about:

- Configuring email alerts
- Configuring network alerts
- Configuring SMS alerts
- Configuring SNMP Traps alerts
- Configuring general settings

To configure Alerting Options:



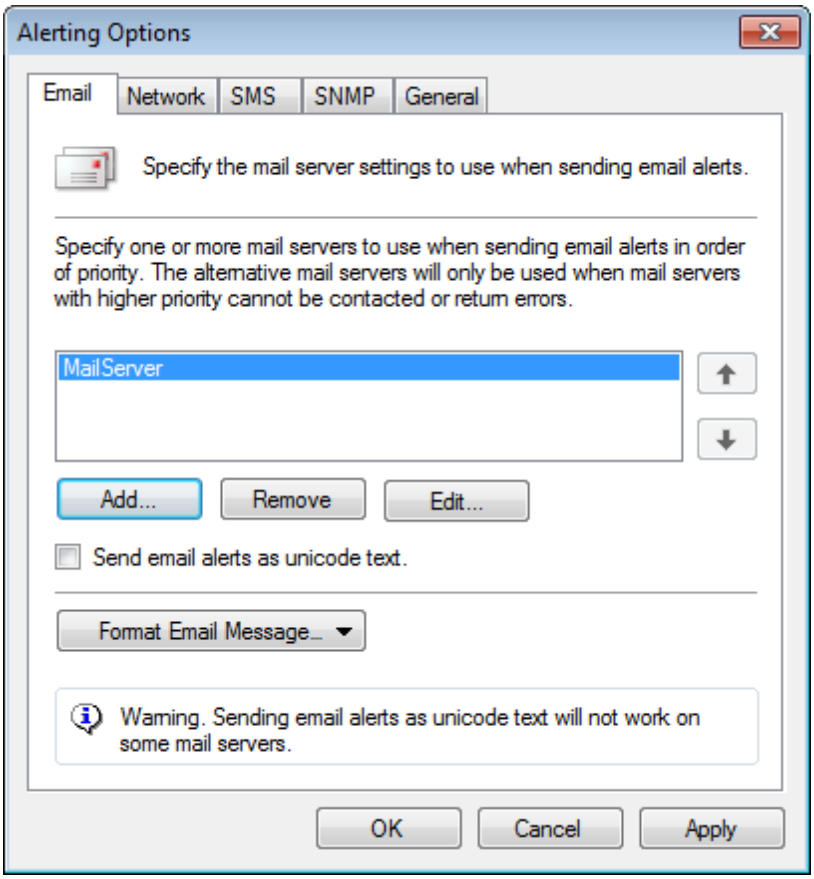
Screenshot 165: Configuring Alerting Options

1. Click **Configuration** tab > **Options**, right-click **Alerting Options** and select **Edit alerting options...**

> **Note**
>
> Select Edit alert recipients to configure the contact details of the alerting recipients and to manage user accounts. For more information refer to Managing user accounts.

2. Configure the alerting method of your choice. The following sections describe how to configure:

11.2.1 Email alerts


Alerting Options
Email
Network
SMS
SNMP
General
Specify the mail server settings to use when sending email alerts.
Specify one or more mail servers to use when sending email alerts in order of priority. The alternative mail servers will only be used when mail servers with higher priority cannot be contacted or return errors.
MailServer
Add...
Remove
Edit...
Send email alerts as unicode text.
Format Email Message...
Warning. Sending email alerts as unicode text will not work on some mail servers.
OK
Cancel
Apply

Screenshot 166: Configuring Email options

To configure email alerts:

1. From the Alerting Options dialog, click **Email** tab.

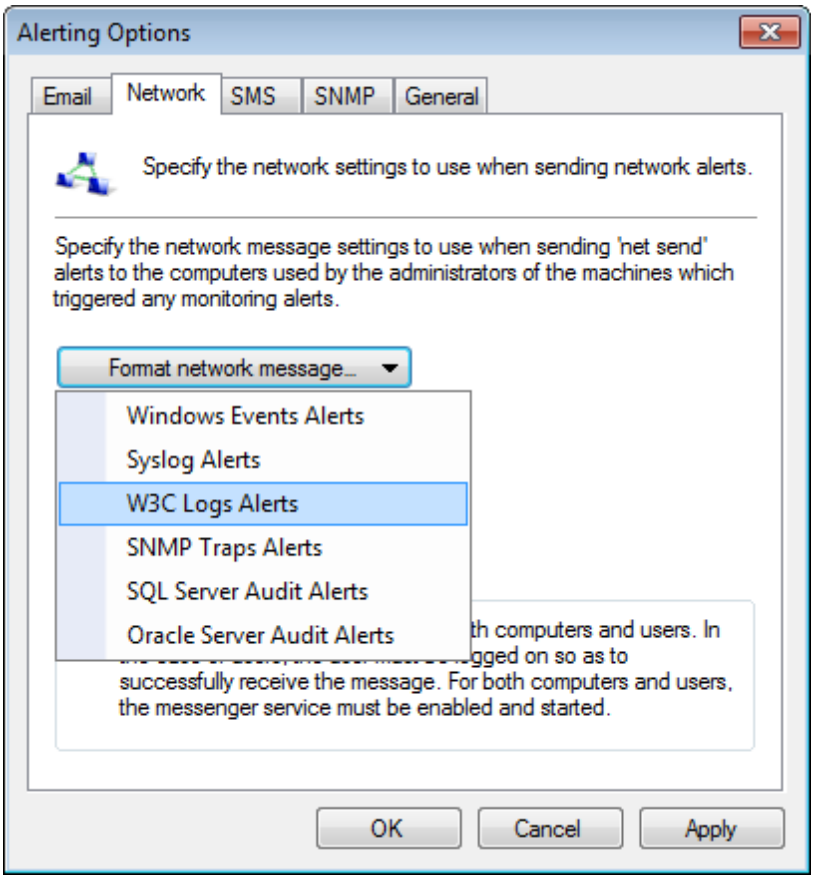
2. Configure the options described below:

Table 75: Alerting Options dialog - Email alerts

Option	Description
Add/Remove/Edit	Click **Add...** to specify the mail server details including the server name /IP, logon credentials and recipient email address. Use the **Remove** or **Edit** button to remove a selected server or edit details.
Up/Down arrow buttons	Use the arrow buttons to change the position of the selected mail server. GFI EventsManager attempts to deliver email alerts via the first mail server. If unsuccessful, it recursively checks the following mail servers.
Send email alerts as Unicode text	Select this option to send emails as Unicode text as opposed to HTML or RTF format.
Format Email Message	Optionally, from the Format Email Message drop-down menu, select the log type (Windows®, Text Logs, Syslog) and customize the email content.

3. Click **Apply** and **OK**.

11.2.2 Network alerts

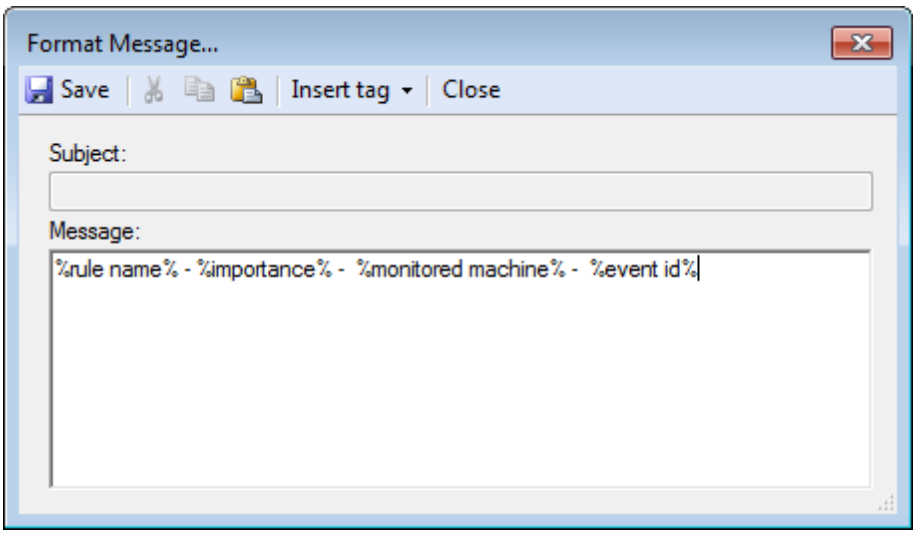

Alerting Options
Email
Network
SMS
SNMP
General
Specify the network settings to use when sending network alerts.
Specify the network message settings to use when sending 'net send' alerts to the computers used by the administrators of the machines which triggered any monitoring alerts.
Format network message...
Windows Events Alerts
Syslog Alerts
W3C Logs Alerts
SNMP Traps Alerts
SQL Server Audit Alerts
Oracle Server Audit Alerts
th computers and users. In
gged on so as to
successfully receive the message. For both computers and users, the messenger service must be enabled and started.
OK
Cancel
Apply

Screenshot 167: Configuring Network options

To configure network alerts:

1. From the Alerting Options dialog, click **Network** tab.

2. From **Format network message…** drop-down menu, select the log type and customize the format of the message.

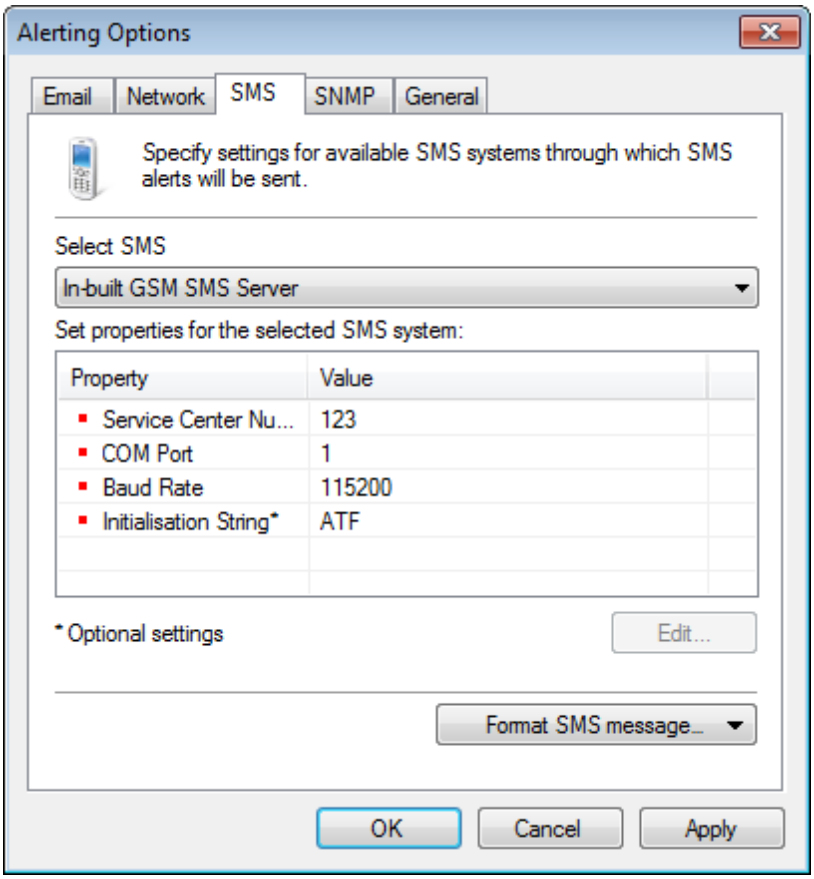


Screenshot 168: Configuring Network alerts: Format message

3. Click **Insert tag** to select from a list of tags to include in the message.

4. Click **Save** and **OK**.

11.2.3 SMS alerts



Screenshot 169: Configuring SMS options

To configure SMS alerts:

1. From the Alerting Options dialog, click **SMS** tab.

2. Configure the options described below:

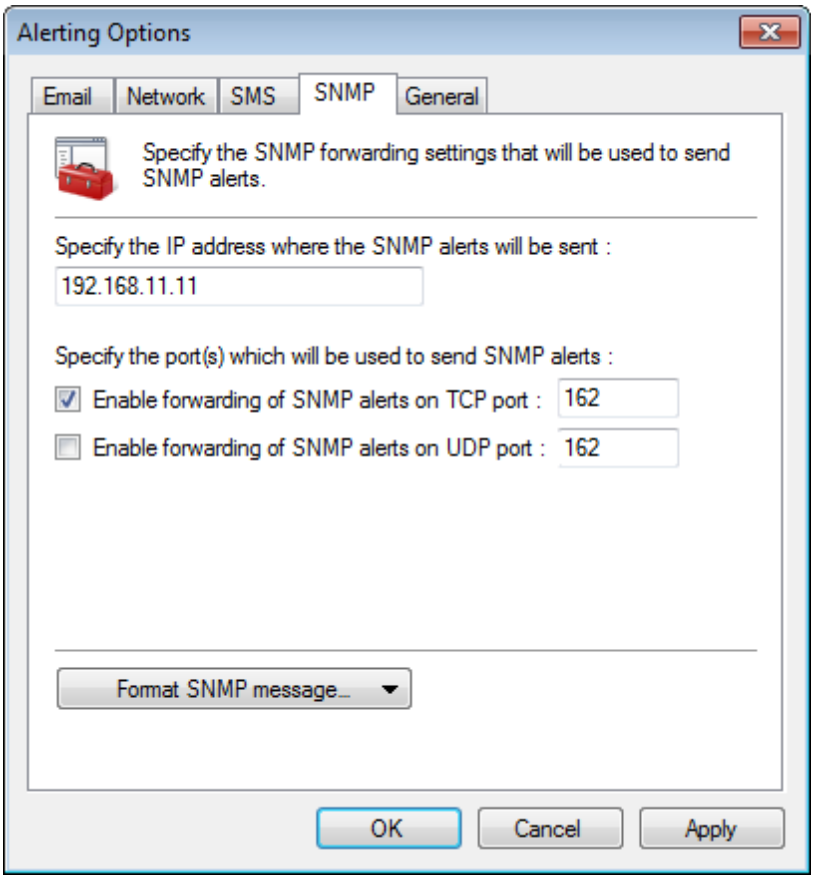
Table 76: Alerting Options dialog: SMS

Option	Description
Select SMS	Select the SMS service used to send SMS alerts. Available services include: » In-built GSM SMS Server » FaxMaker SMS service provider template » Clickatell Email2SMS Service » Generic SMS service provider template.
Set properties for the selected SMS system	Configure the properties for the selected SMS service type. Amongst others, property settings include: » Service center number » COM Port » Baud Rate » SMTP Server » SMTP Port. Click **Edit...** to configure the selected property.
Format SMS message	Optionally, from the **Format Email Message** drop-down menu, select the log type (Windows®, Text Logs, Syslog) and customize the email content.

3. Click **Apply** and **OK**.

11.2.4 SNMP alerts

To configure SNMP alerts:



Screenshot 170: Configuring SNMP alerts

1. From the **Alerting Options** dialog, click **SNMP** tab.
2. Configure the options described below:

Table 77: Alerting Options: SNMP Traps

Option	Description
Specify the IP address where the SNMP alerts will be sent	Enter the IP address of the recipient.
Specify the port(s) which will be used to send SNMP alerts	Specify TCP/UDP communication port. By default, the assigned port is 162.
Format SNMP message	Optionally, from the Format Email Message drop-down menu, select the log type (Windows®, Text Logs, Syslog) and customize the email content.

3. Click **Apply** and **OK**.

11.2.5 General settings

To configure general alerts settings:

1. From the **Alerting Options** dialog, click **General** tab.
2. Configure the options described below and click **OK**:

Table 78: Alerting Options: General settings

Option	Description
Send email alerts on database errors	Email alerts are sent upon database errors such as backup failure, data corruption, size exceeds maximum size specified and other database operation errors.

12 User Groups

This chapter provides you with information related to creating and managing users and groups. Through the Users and Groups node, users and groups can be created and specific alerts, working hours and other properties can be assigned to each user and group; while different console access rights can be assigned to each user from the Console Security and Audit Options node.

Topics in this chapter:

12.1 Configuring the administrator account 216

12.2 Managing user accounts 222

12.3 Managing user groups 229

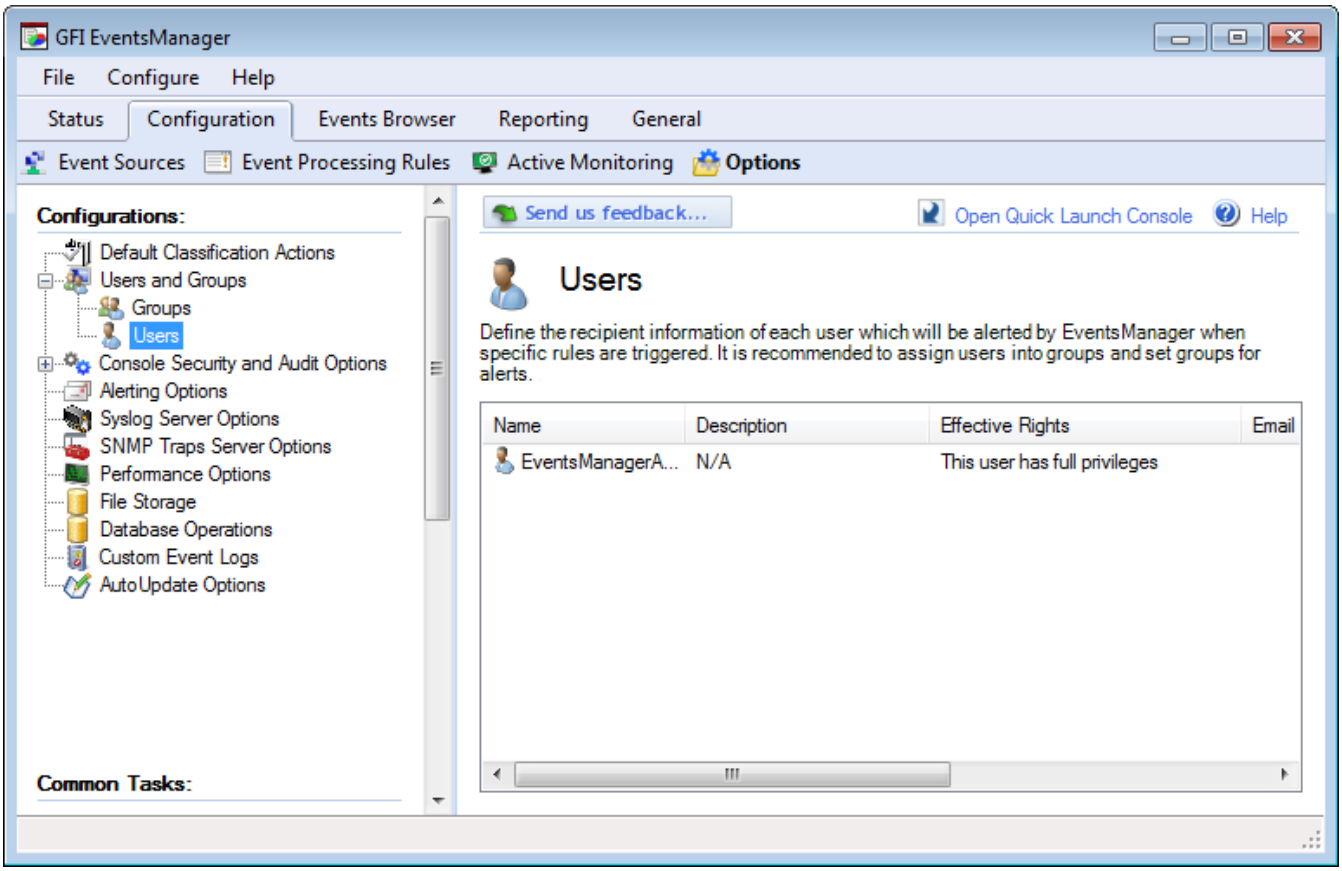
12.1 Configuring the administrator account

GFI EventsManager automatically creates an **EventsManagerAdministrator** account. However, you must still configure some properties such as the notification addresses and account security.

> **Note**
>
> GFI EventsManager requires a valid administrator email address in order to distribute automatic alerts when particular events are discovered.

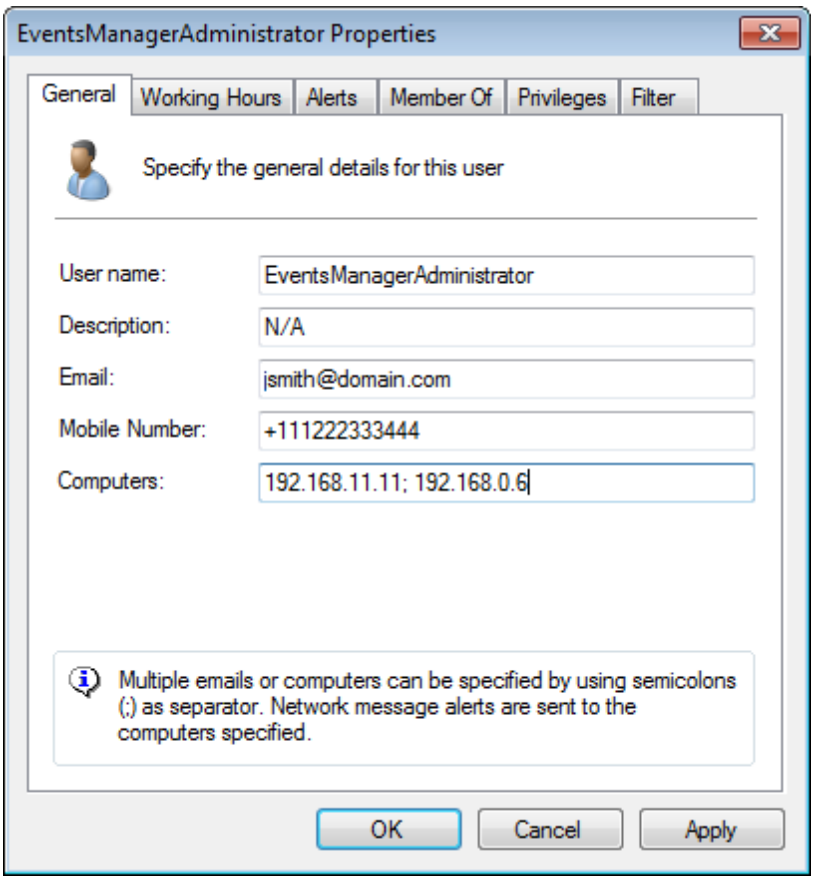
To configure the GFI EventsManagerAdministrator account:

1. From **Configuration** tab > **Options**, expand **Users and Groups** > **Users**.



Screenshot 171: Configuring EventsManagerAdministrator account

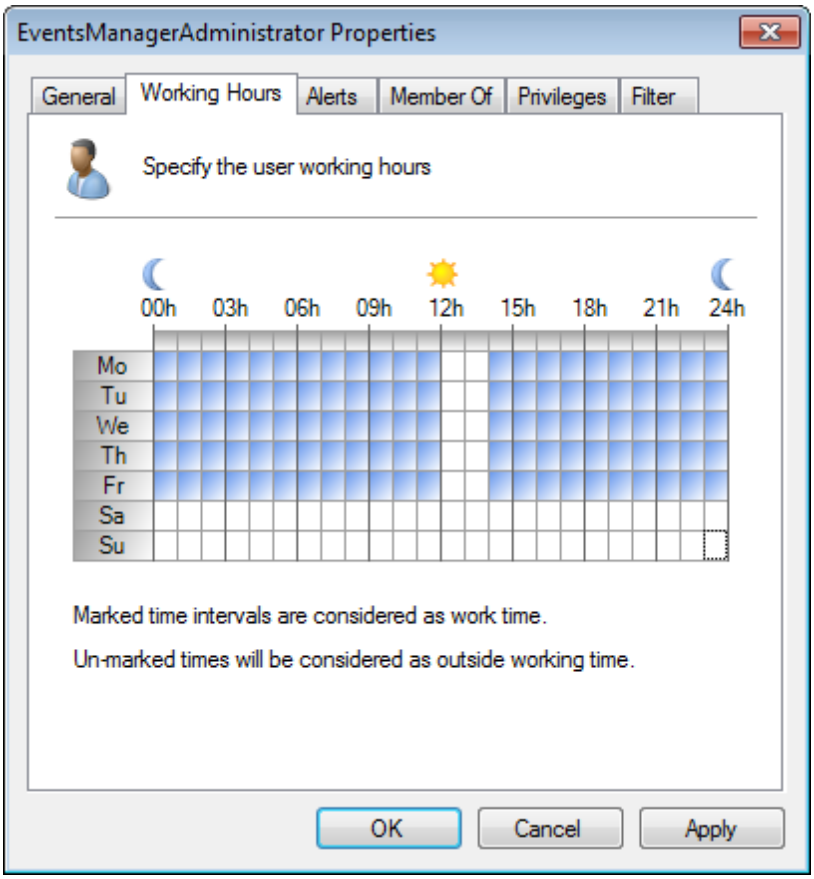
2. From the right pane, right-click **EventsManagerAdministrator** and click **Properties.**



Screenshot 172: EventsManagerAdministrator properties

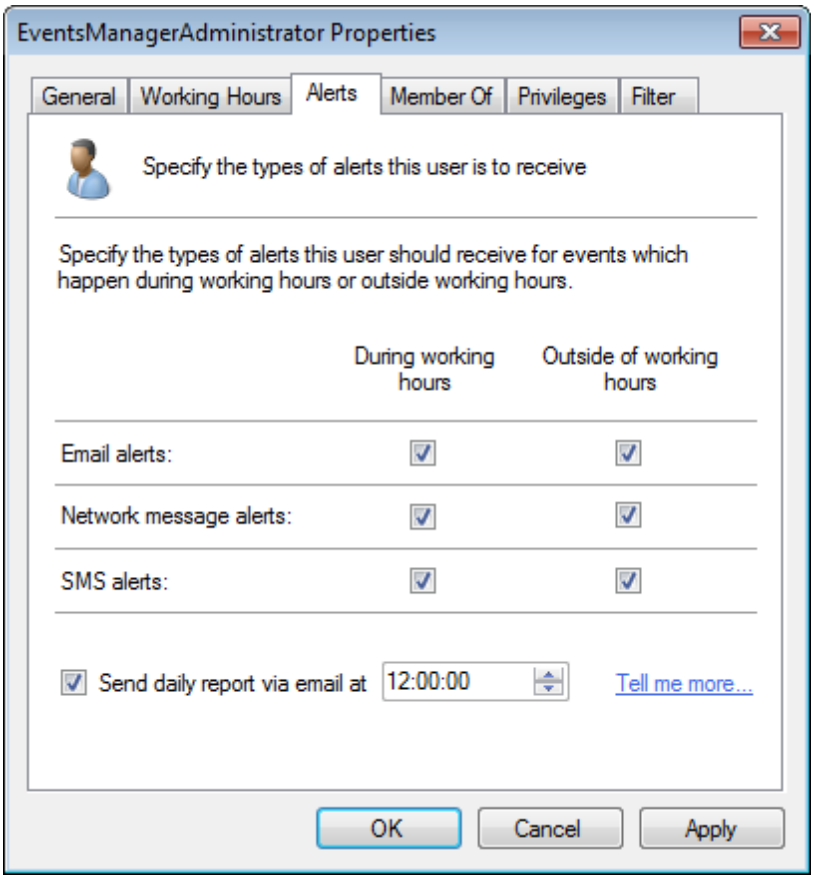
3. From the **General** tab specify:

- A username for GFI EventsManager administrator account
- (Optional) A description for the account
- A valid email address for email alerts distribution
- A valid mobile number for SMS alerts distribution
- Valid computer names/IPs for network alerts distribution.



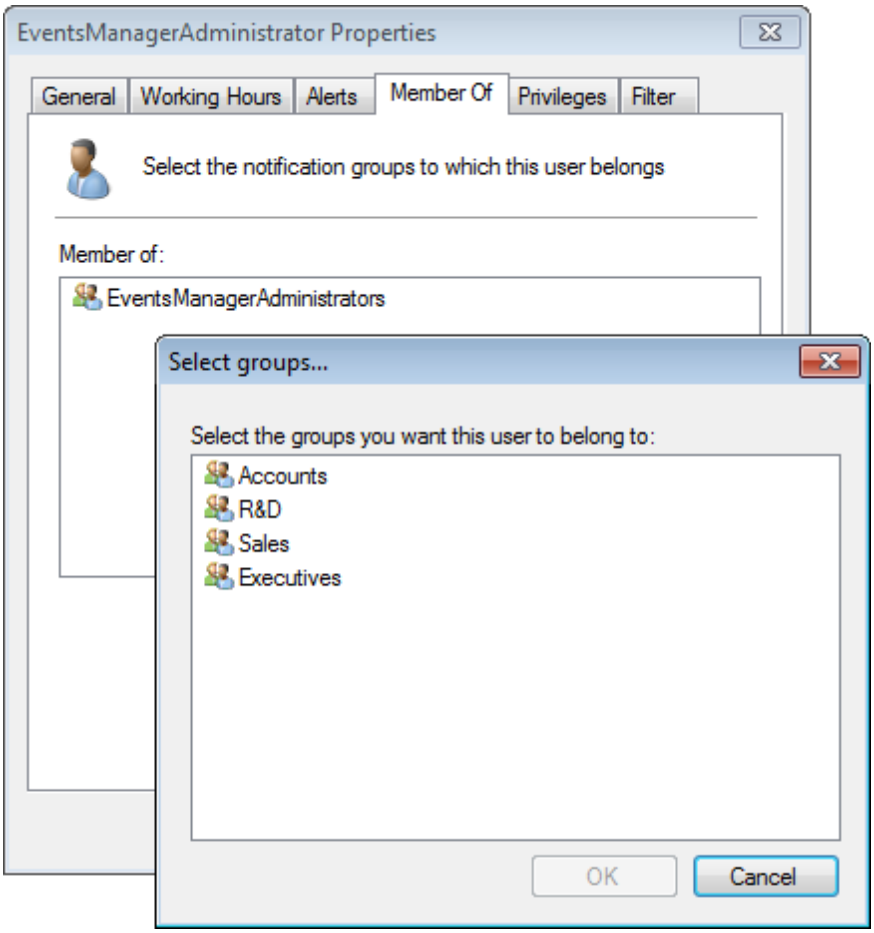
Screenshot 173: Configuring user typical working hours

4. Click **Working Hours** tab and specify the typical working hours of the administrator. Marked time intervals are considered as working hours.



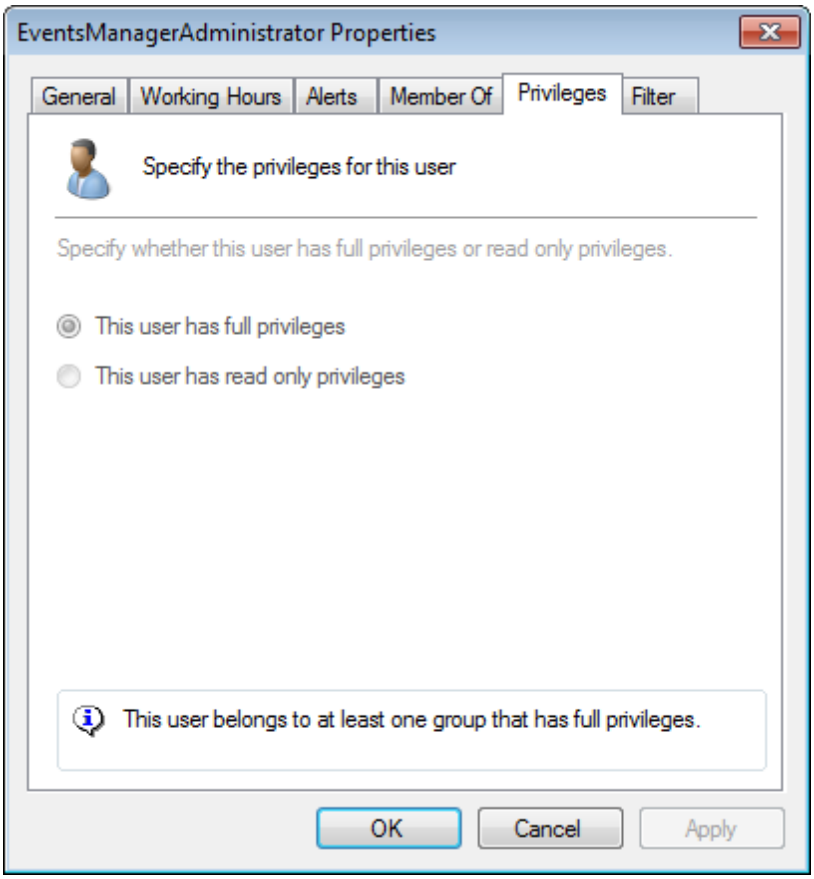
Screenshot 174: Configure alerts outside working hours

5. Click **Alerts** tab and select the alerts sent during and outside working hours. Optionally, select **Send daily report via email at** and specify the time to send an email containing daily activity.



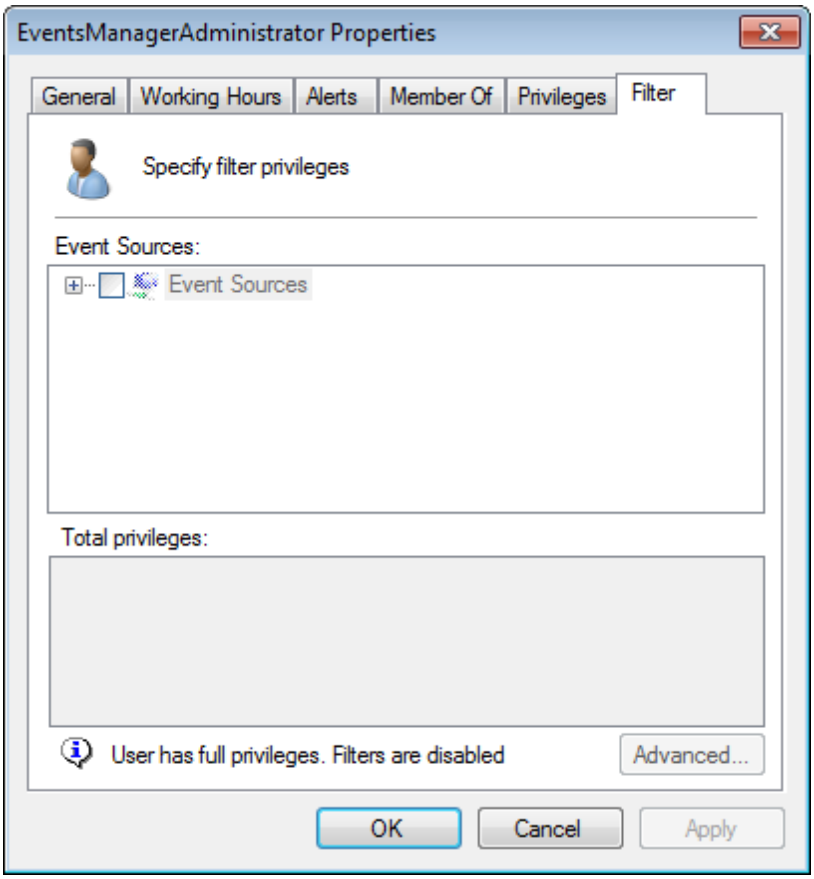
Screenshot 175: Select the group which the user account is a member of

6. Click **Member Of** tab and select the notification groups to which the user belongs. By default the administrator is a member of the **EventsManagerAdministrators** notification group.



Screenshot 176: Configuring user account privileges

7. Click **Privileges** tab to edit the user privileges. By default the EventsManagerAdministrator account has full privileges and cannot be modified.



Screenshot 177: User account filtering

8. Click **Filter** tab to edit what the administrator can see in the management console. By default, this tab is disabled for the EventManagerAdministartor account.

9. Click **Apply** and **OK**.

12.2 Managing user accounts

GFI EventsManager allows you to create a custom list of users which you can organize into groups to speed up administrative tasks.

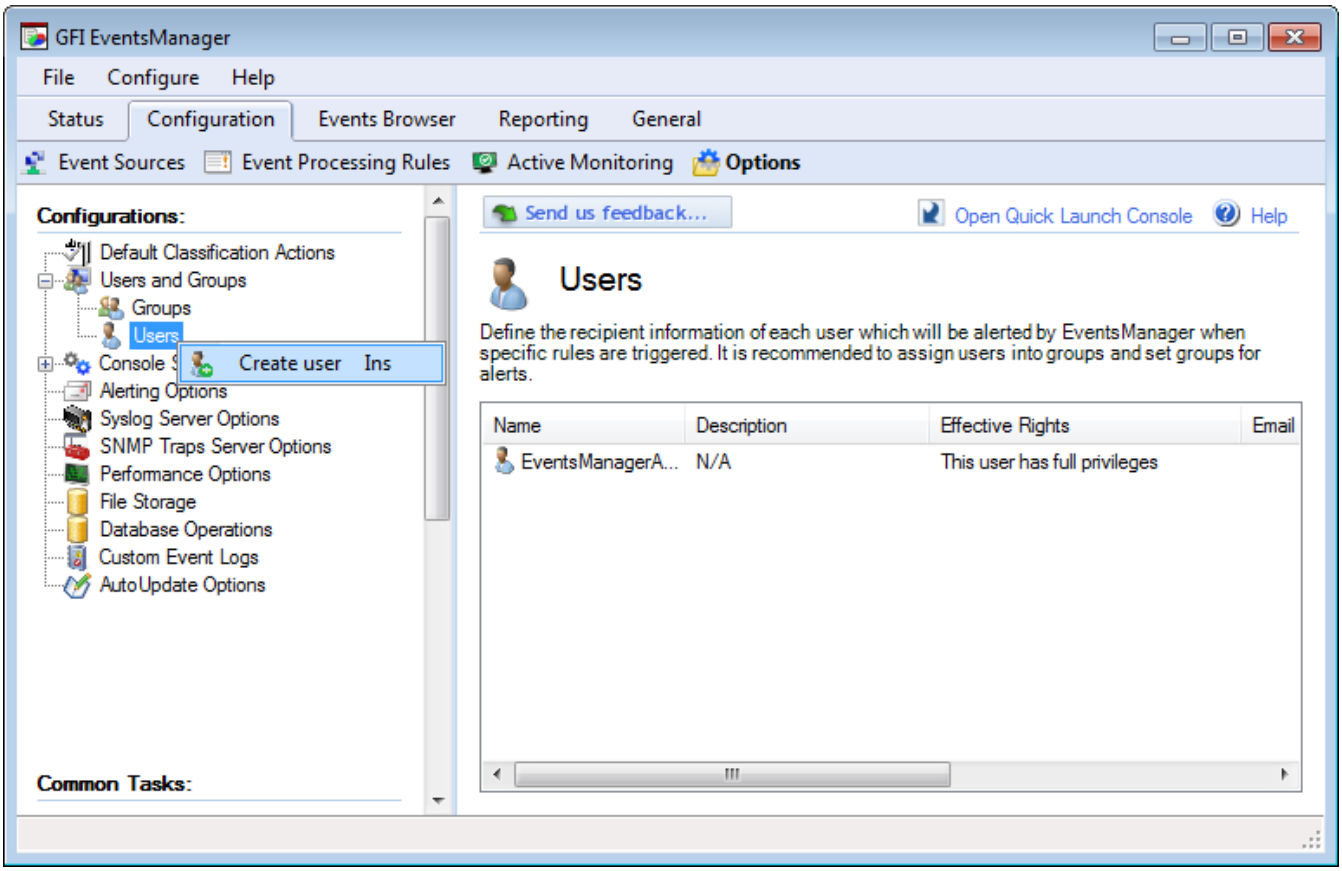
This section contains information about:

- Creating a new user account
- Changing user account properties
- Deleting a user account

12.2.1 Creating a new user account

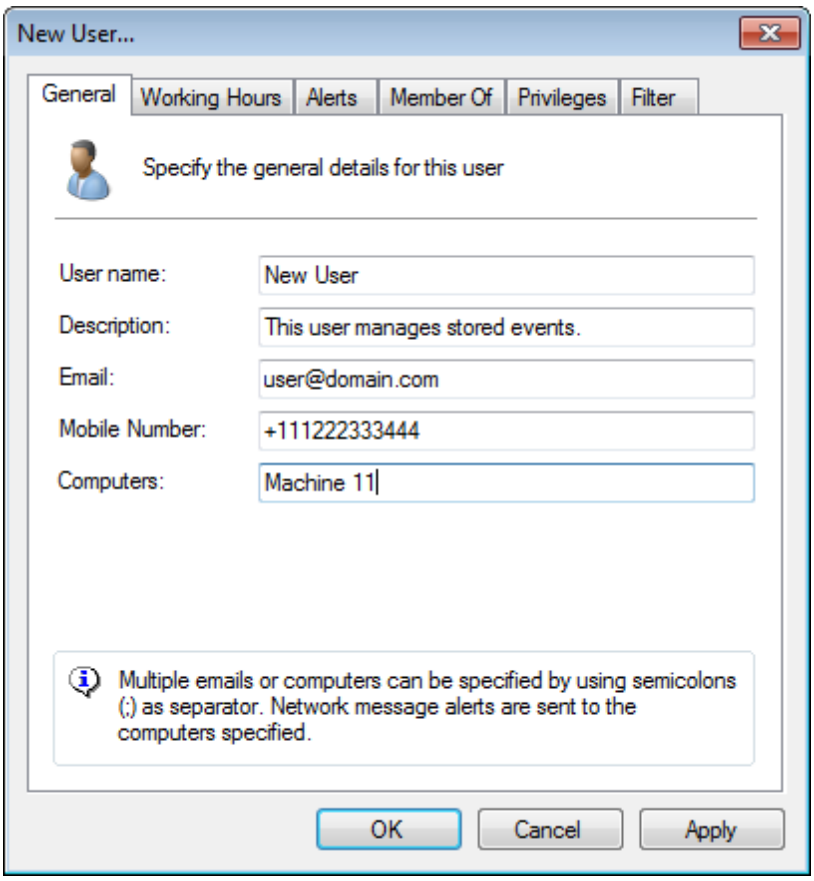
To create a new user:

1. From **Configuration** tab > **Options**, expand the **Users and Groups** node.



Screenshot 178: Creating a new user

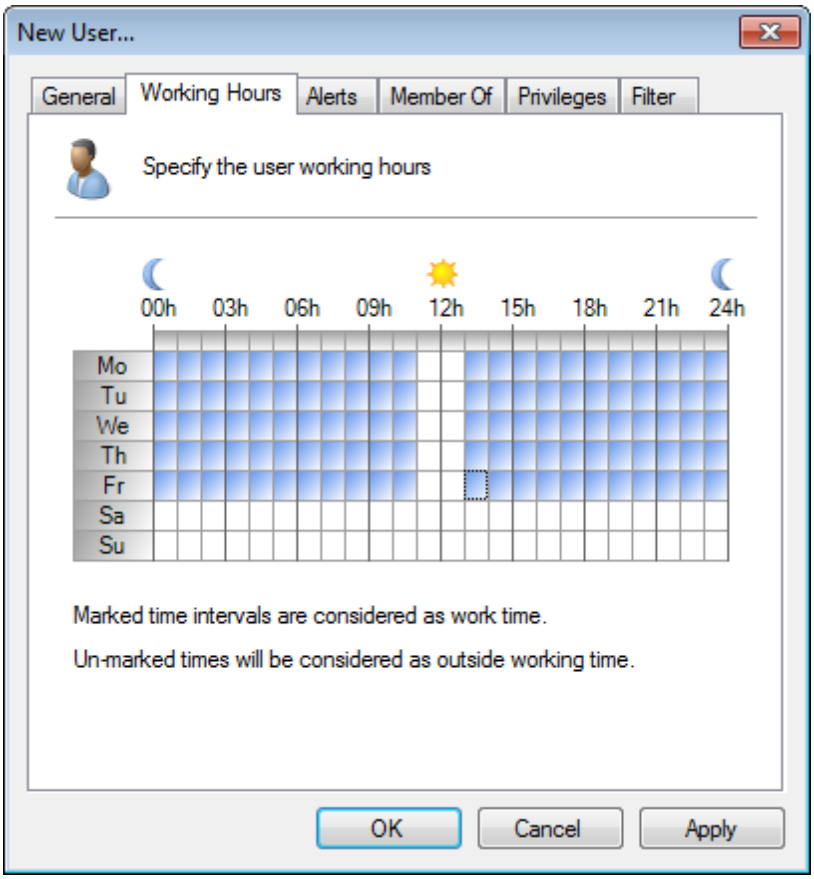
2. Right-click **Users** sub-node and select **Create user...**



Screenshot 179: Creating a new user - General properties

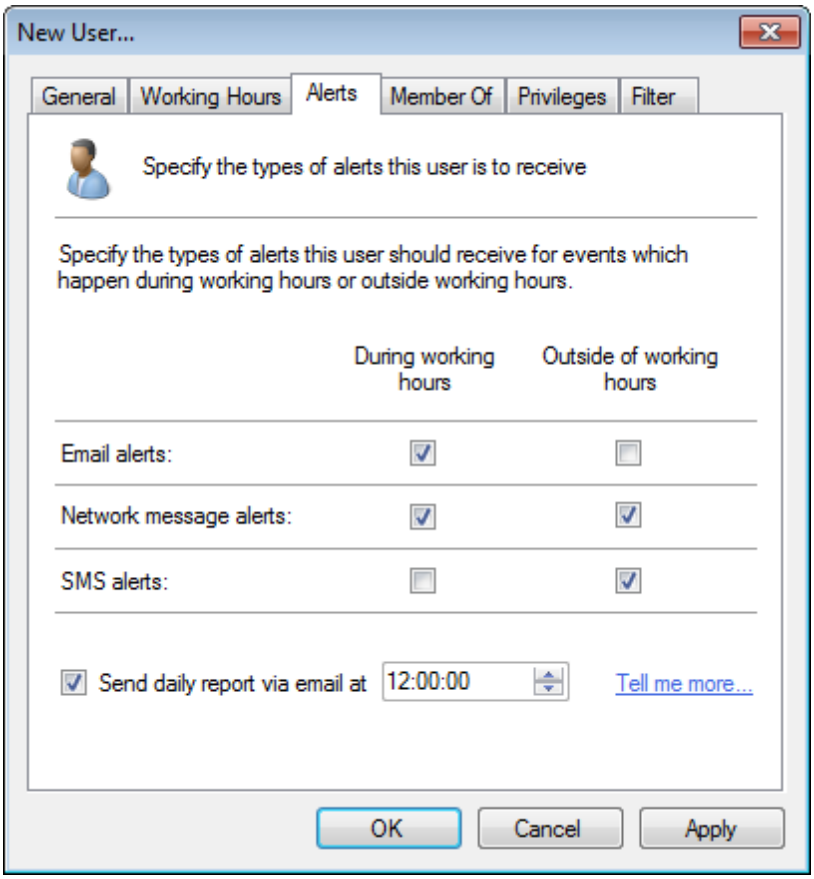
3. From the **General** tab specify:

- A username for the user account
- (Optional) A description for the account
- A valid email address for email alerts distribution
- A valid mobile number for SMS alerts distribution
- Valid computer names/IPs for network alerts distribution.



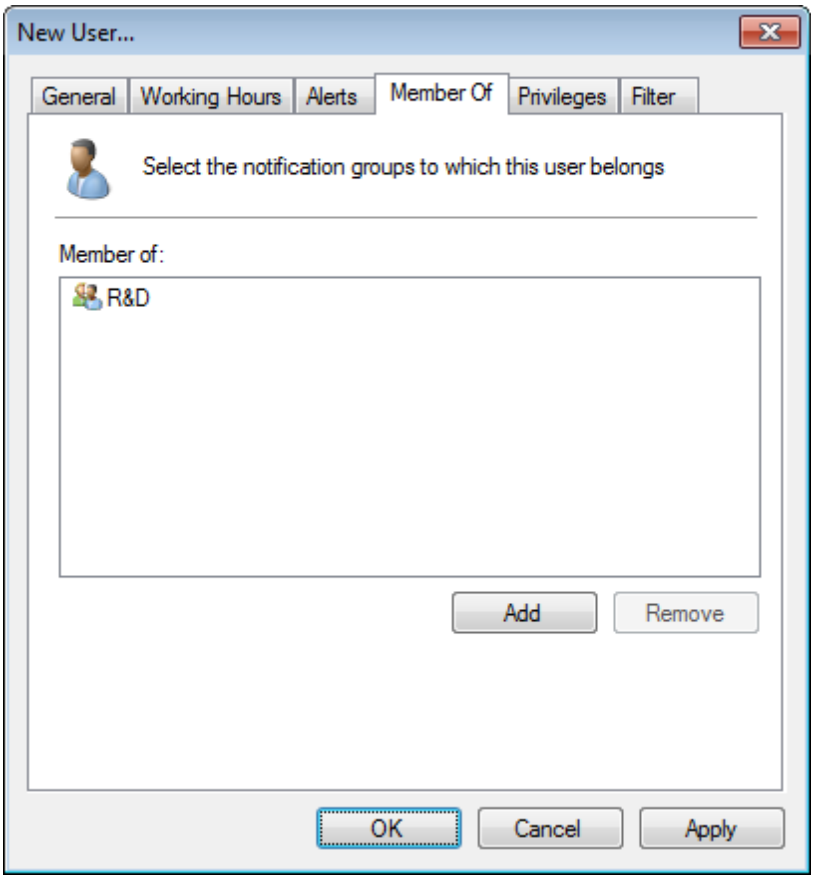
Screenshot 180: Creating a new user - Working hours

4. Click **Working Hours** tab and specify the typical working hours of the new user. Marked time intervals are considered as working hours.



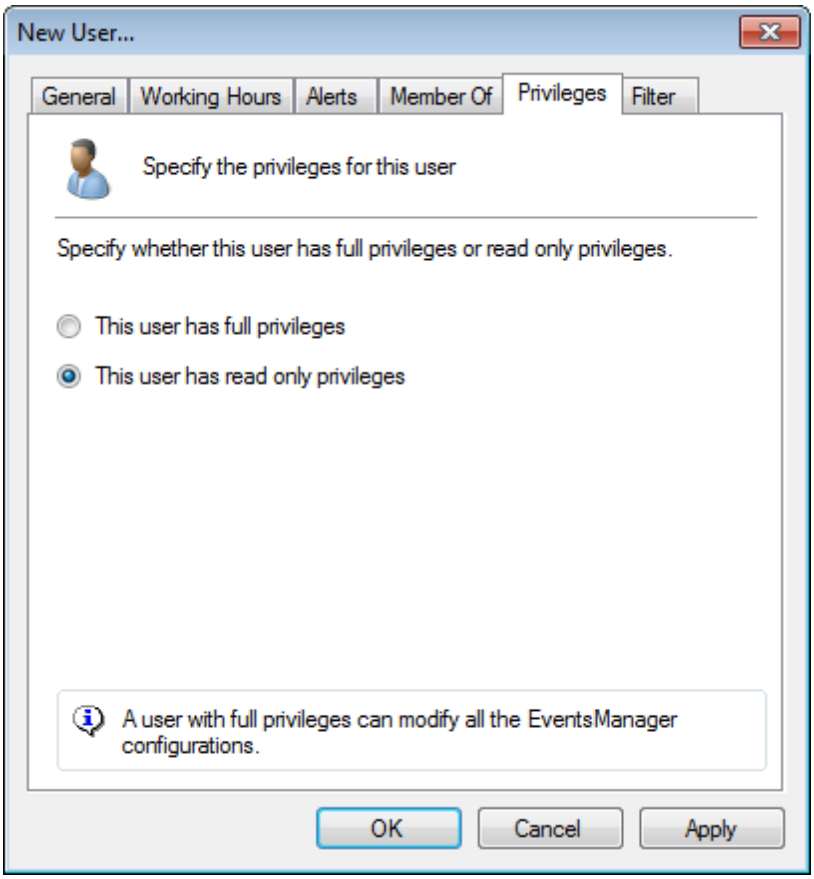
Screenshot 181: Creating a new user - Alerting options

5. Click **Alerts** tab and select the alerts sent during and outside working hours. Optionally, select **Send daily report via email at** and specify the time to send an email containing daily activity. For more information, refer to Alerts and Default Actions (page 208).



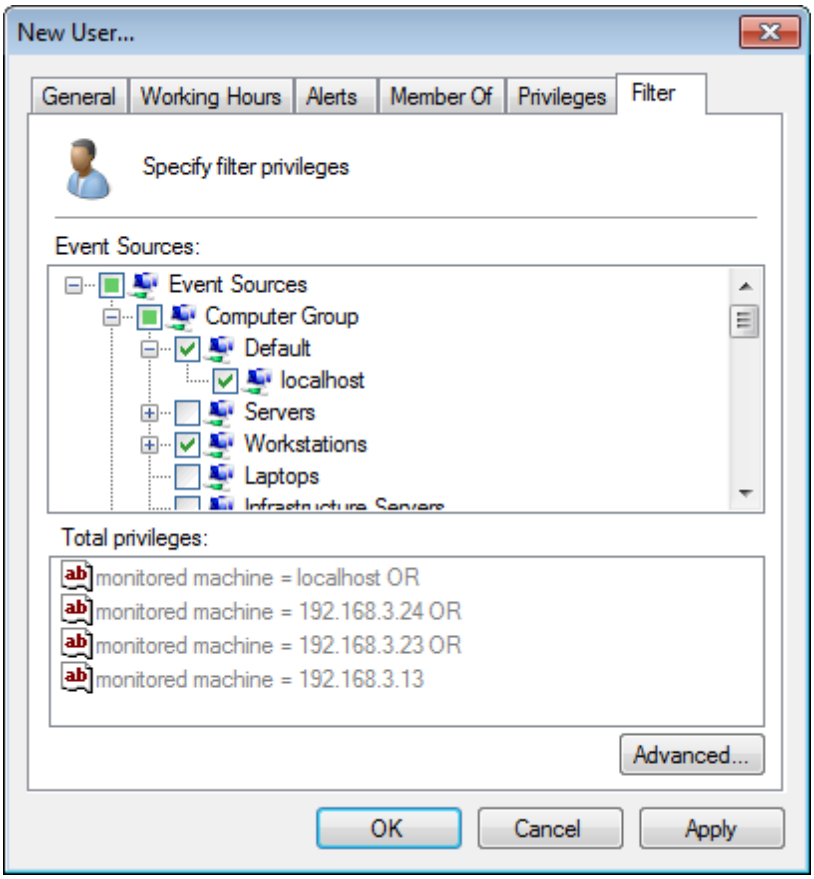
Screenshot 182: Creating a new user - Select notification group(s)

6. Click **Member Of** tab and click **Add**. Select the notification groups to which the user belongs and click **OK**.



Screenshot 183: Creating a new user - Privileges

7. Click **Privileges** tab to configure user privileges. By default, new user accounts have read only privileges.



Screenshot 184: User filtering options

8. Click **Filter** tab to configure what the new user is allowed to display in the management console. The following table describes the available options:

Table 79: User filtering options

Option	Description
Event Sources	GFI EventsManager provides you with a set of pre-configured conditions for filtering event sources. Select the event sources that you want to be visible for this user.
Total privileges	Click **Advanced...** to launch the **Advanced Filtering** dialog. This dialog enables you to build your own conditions for granular filtering, allowing you to filter events containing specific attributes. To add a condition: 1. From the **Advanced Filtering** dialog, click **Add** and select a field from the list. Example: Date, Importance, Log format. 2. For the selected field, select an operator from the **Field operator** drop-down menu. Example: Equal to, Less than, Greater than. 3. Specify a value for the operator in the **Field value** text box. 4. Click **OK**. 5. Repeat steps 1 to 4 to add more than one field name. **Note** For more information refer to Defining query restrictions.

9. Click **Apply** and **OK**.

12.2.2 Changing user account properties

To edit user properties:

1. From **Configuration** tab > **Options**, expand the **Users and Groups** node.

2. From **Users** sub-node, right-click a user and select **Properties**.

3. Make the required changes in the tabs available and click **OK**.

12.2.3 Deleting a user account

To delete a user:

1. From **Configuration** tab > **Options**, expand the **Users and Groups** node and select **Users**.

2. From right pane, right-click a user and select **Delete**.

12.3 Managing user groups

GFI EventsManager enables you to assign users to a group. Once the group properties have been configured, every member of the group inherits the same settings.

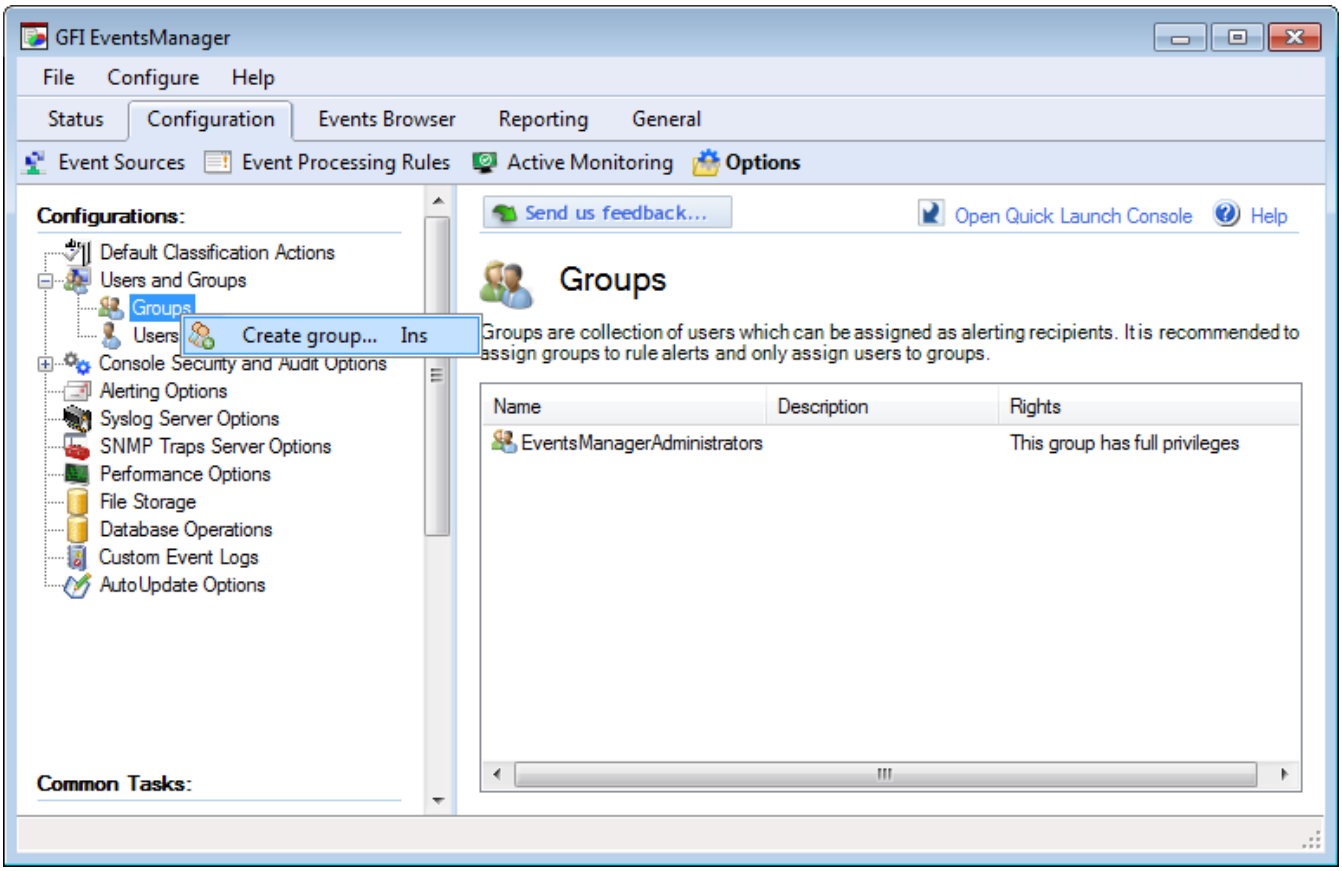
This section contains information about:

- Creating a new group
- Changing group properties
- Deleting a group

12.3.1 Creating a new group

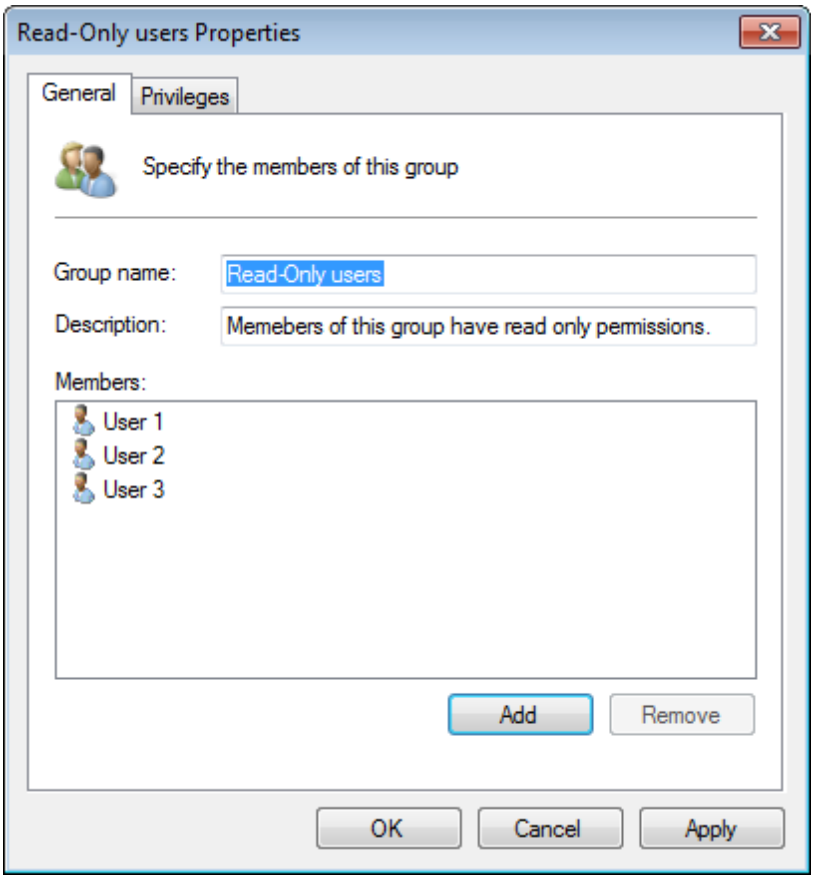
To create a new user group:

1. From **Configuration** tab > **Options**, expand **Users and Groups** node.



Screenshot 185: Creating a new user group

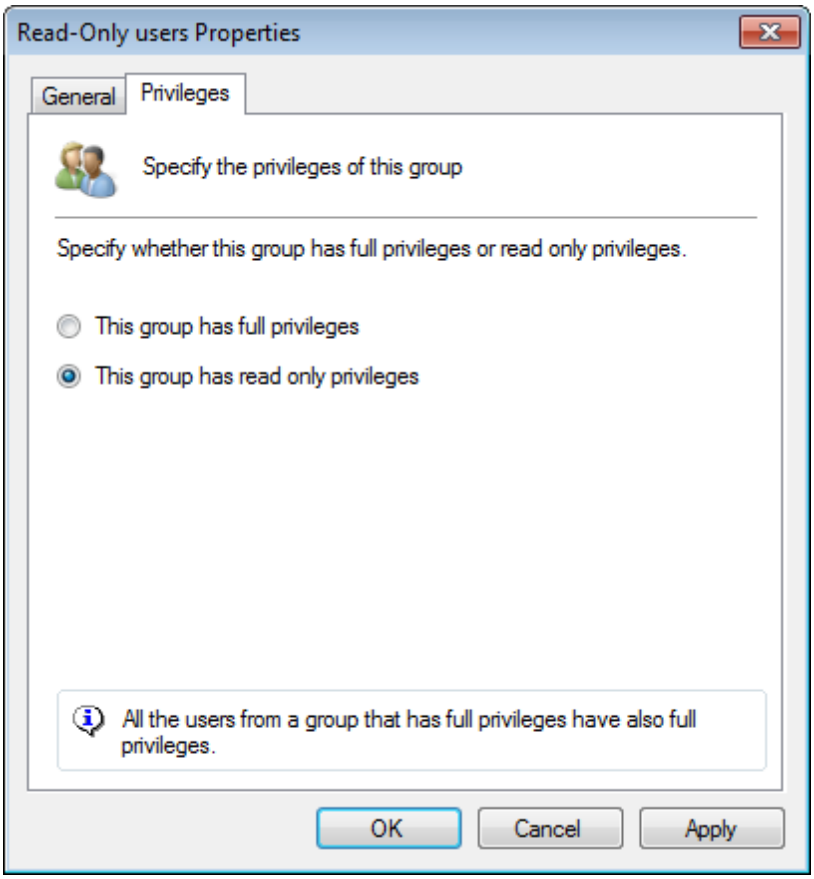
2. Right-click **Groups** sub-node and select **Create group…**



Screenshot 186: Creating a new user group - General properties

3. Specify the name and an optional description for the new group.

4. Click **Add** to add users to the group.


Read-Only users Properties
General
Privileges
Specify the privileges of this group
Specify whether this group has full privileges or read only privileges.
This group has full privileges
This group has read only privileges
All the users from a group that has full privileges have also full privileges.
OK
Cancel
Apply

Screenshot 187: Creating a new user group - General properties

5. From the **Privileges** tab, select if the group has **Full** or **Read Only** permissions.

6. Click **Apply** and **OK**.

12.3.2 Changing group properties

To edit the settings of a user group:

1. From **Configuration** tab > **Options**, expand **Users and Groups** node.

2. From the right pane, right-click on the group to be configured and select **Properties**.

3. Perform the required changes in the tabs available and click **OK**.

12.3.3 Deleting a group

To delete a user group:

1. From **Configuration** tab > **Options**, expand **Users and Groups** node.

2. Right-click on the group to be deleted and select **Delete**.

13 Console Security and Audit Options

Console security and audit options enable you to protect GFI EventsManager from unauthorized access and malicious intent. The provided audit options enable you to accurately monitor GFI EventsManager activity.

Topics in this chapter:

13.1 Enabling login system 232

13.2 Anonymization 235

13.3 Auditing console activity 238

13.4 Auto-discovery credentials 239

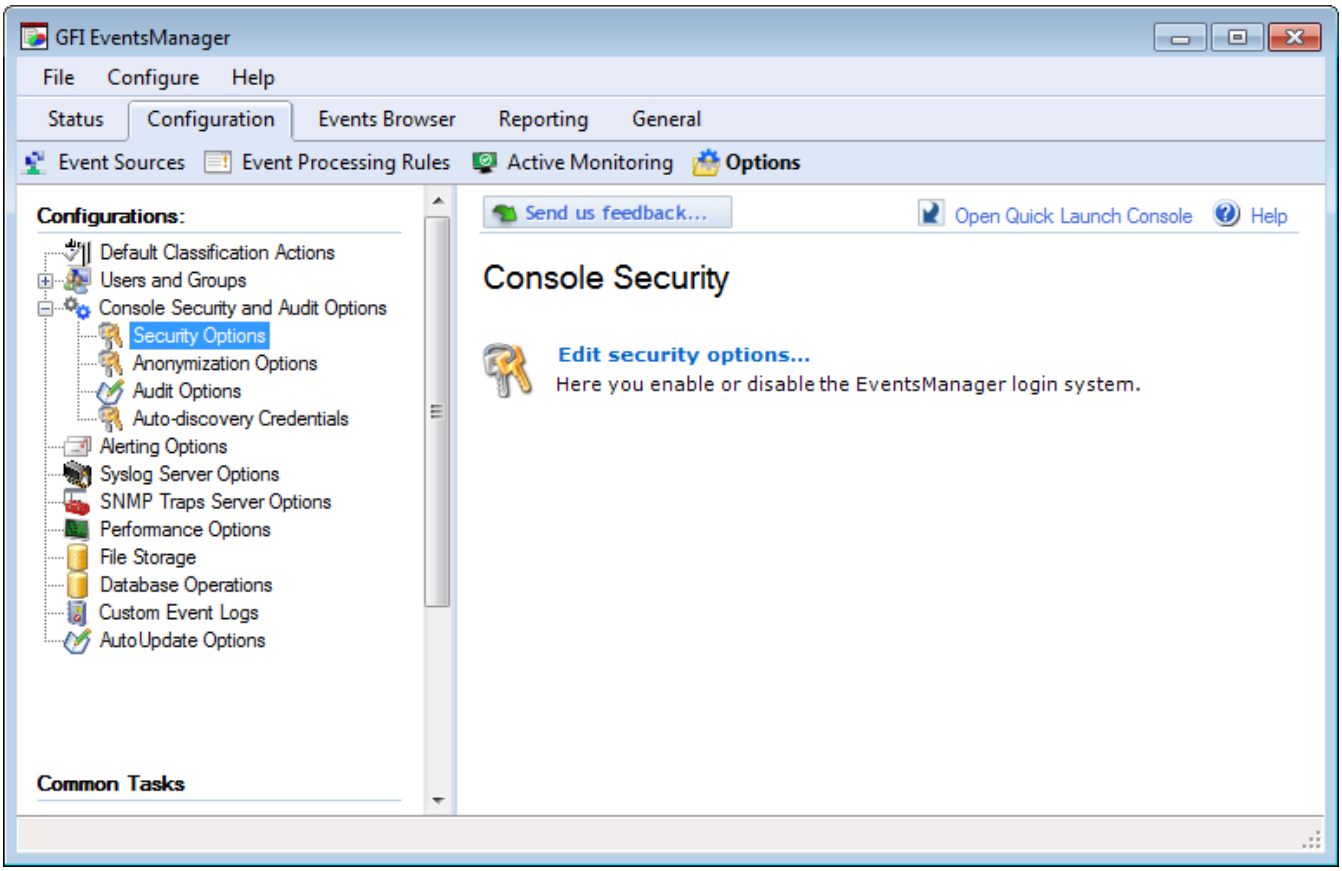
13.1 Enabling login system

When the login system is enabled all users will be asked to specify their credentials every time they launch the GFI EventsManager management console.

> **Note**
>
> Before you enable the login system, you must configure your mail server settings. For more information refer to Configuring Alerting Options.

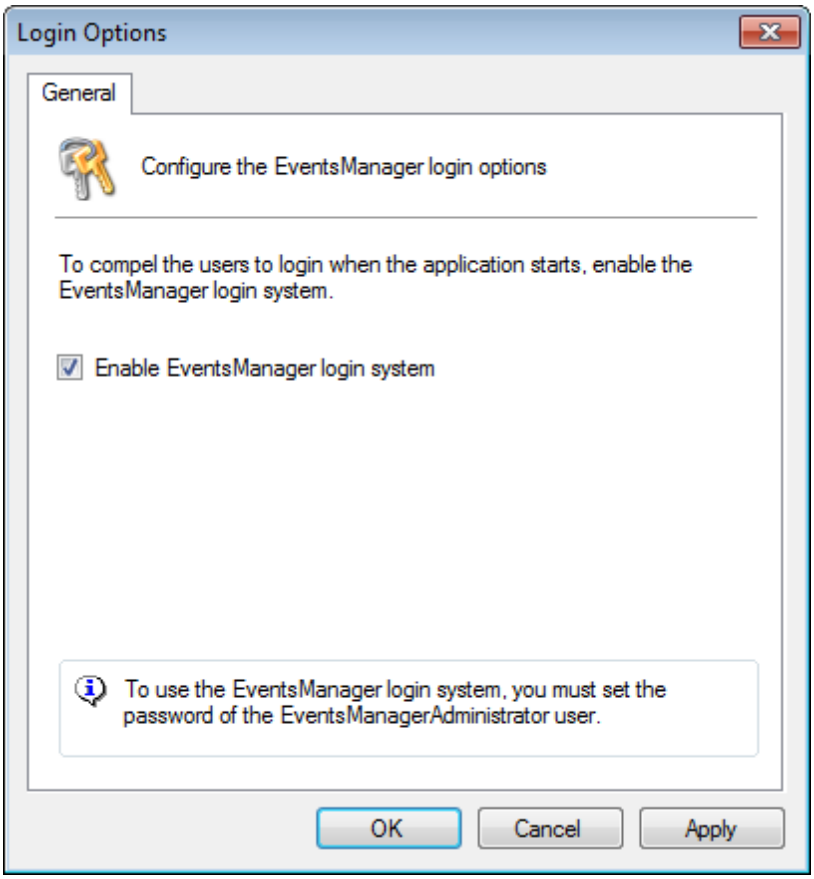
To enable the log-in system:

1. From **Configuration** tab > **Options** expand **Console Security and Audit Options** node.



Screenshot 188: Editing console security options

2. Expand **Console Security and Audit Options** node, right-click **Security Options** node and select **Edit security options...**.


Login Options
General
Configure the EventsManager login options
To compel the users to login when the application starts, enable the EventsManager login system.
Enable EventsManager login system
To use the EventsManager login system, you must set the password of the EventsManagerAdministrator user.
OK
Cancel
Apply

Screenshot 189: Enabling EventsManager login system

3. Select **Enable EventsManager login system** to enable login.

4. Click **Apply** and **OK**.

Note

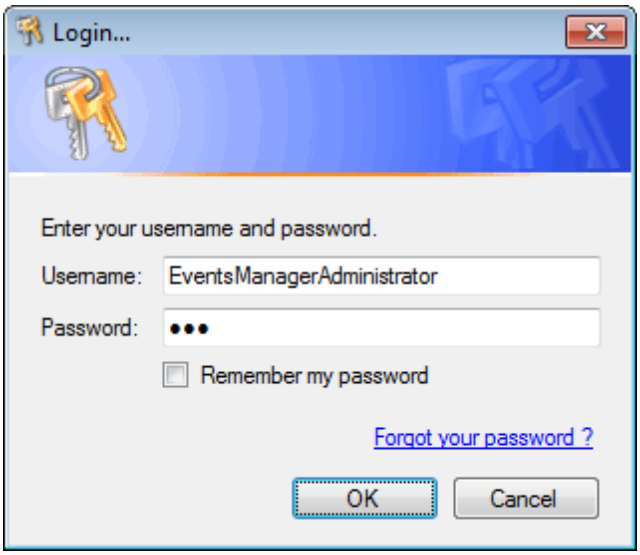
To configure or edit user passwords go to **Configuration** tab > **Users and Groups** > **Users**, right-click the user account and select **Change Password**.

Important

Once the login system is enabled, users must login to the console by specifying their username and password and must have a valid email configured to be able to retrieve lost passwords. For more information refer to Managing user accounts.

13.1.1 Password recovery

When GFI EventsManager login system is enabled, all users are requested to enter a valid user name and password to access the management console.



Screenshot 190: Login credentials prompt

If a password is forgotten or lost:

1. Key in your username.

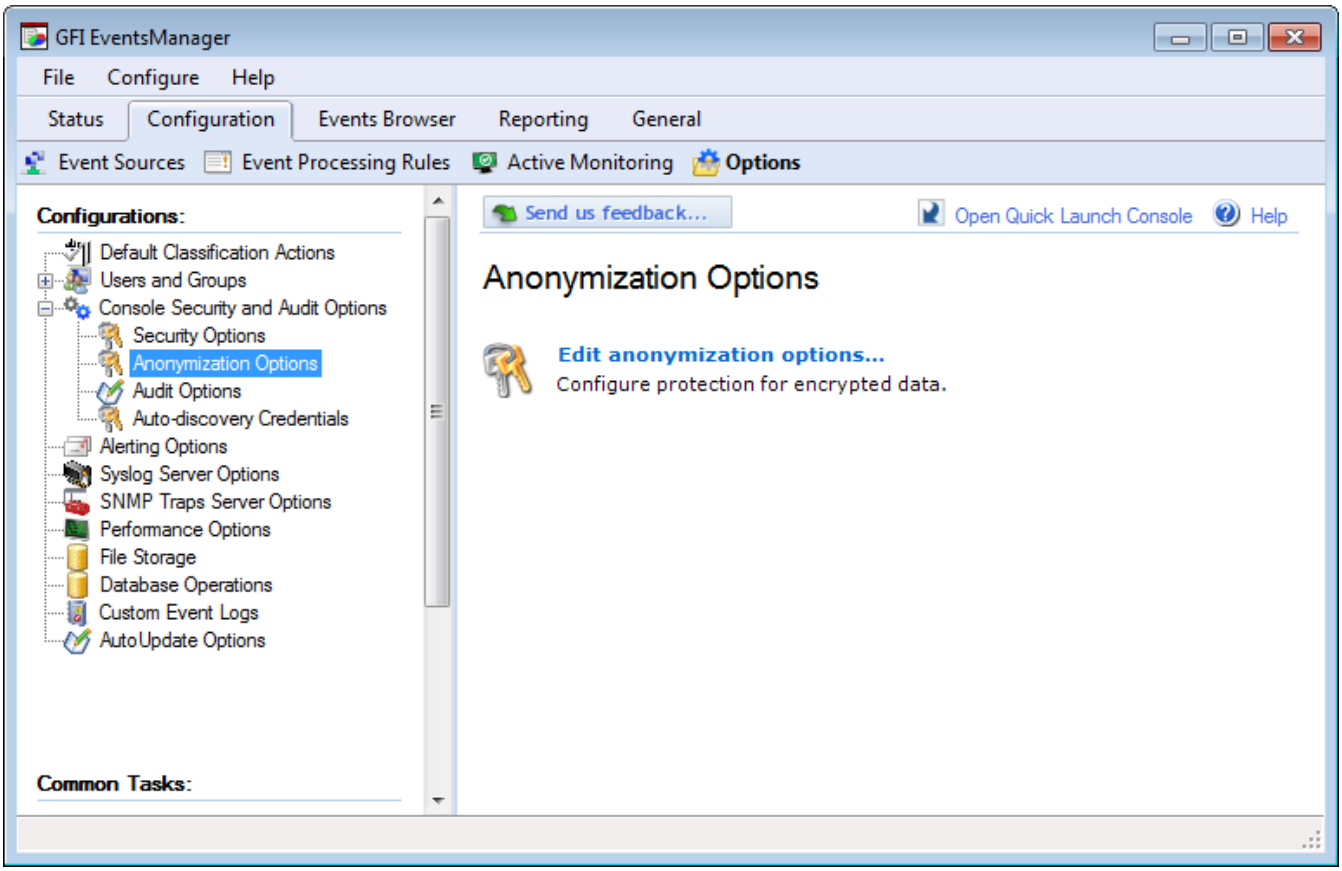
2. Click **Forgot your password?** link. GFI EventsManager will send an email containing your login password on the email address supplied during the user account setup.

13.2 Anonymization

In some countries privacy laws state that it is against the law not to encrypt personal information retrieved by monitoring applications for privacy protection. GFI EventsManager enables you to encrypt personal information when exporting and/or viewing event logs.

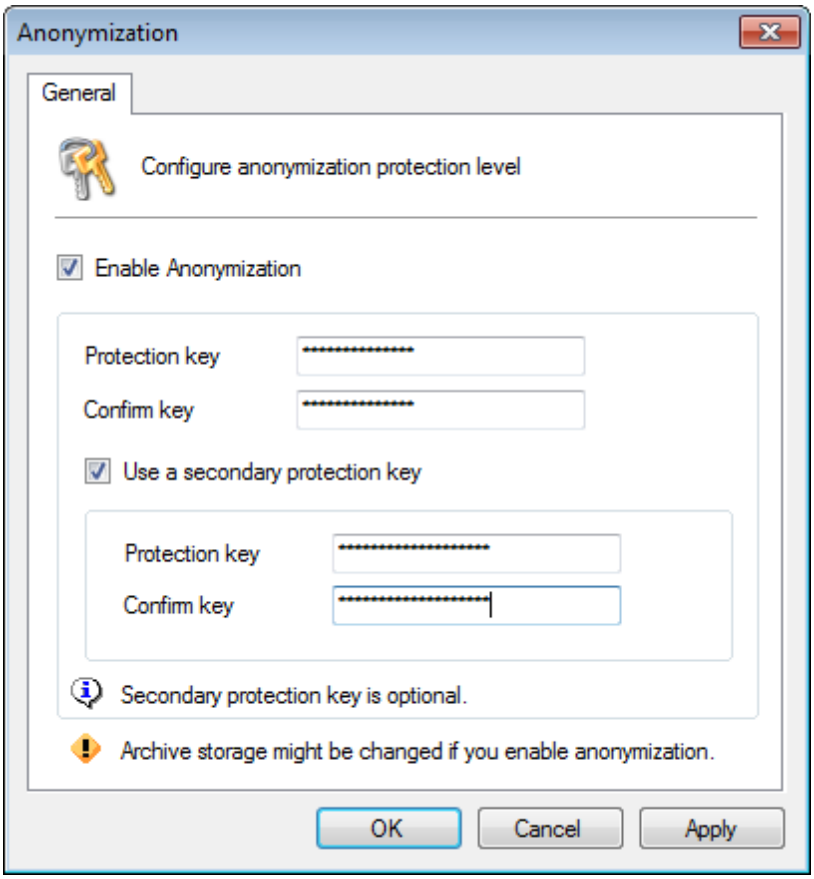
Enable anonymization to encrypt all personal information. The Events Browser and Dashboard can recognize such information and do not display it. Instead, they display **<encrypted>** or **Anonymized data** messages instead.

To configure anonymization:



Screenshot 191: Enable console anonymization

1. From **Configuration** tab > **Options**, expand **Console Security and Audit Options** node, right-click **Anonymization** and click **Edit anonymization options…**



Screenshot 192: Anonymization options

2. Select **Enable Anonymization** and enter the encryption password.

3. (Optional) Select **Use a secondary protection key** to use two passwords for event log encryption. Event logs can only be decrypted by providing two decryption passwords.

4. Click **Apply** and **OK**.

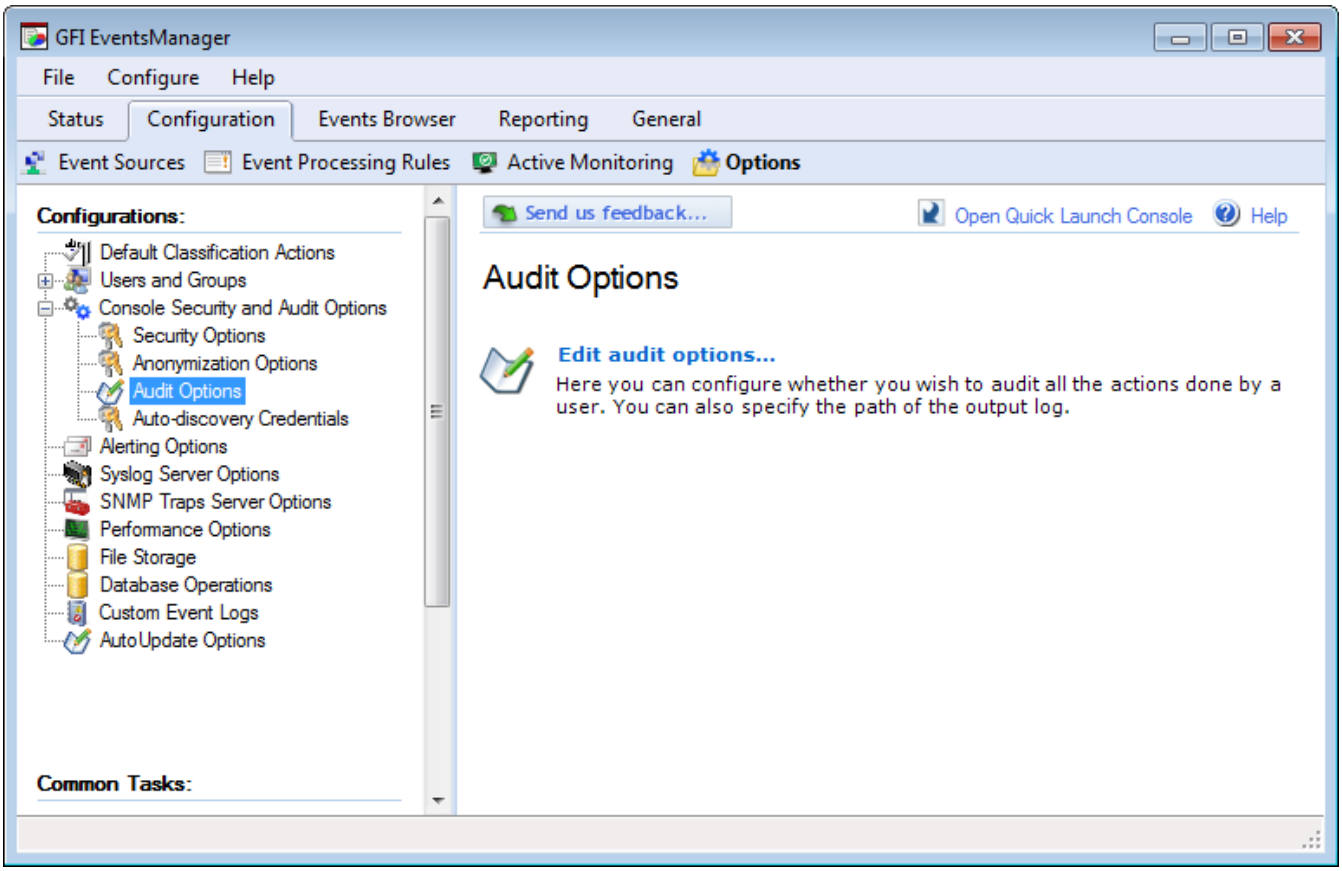
Note

Once anonymization is enabled, personal data is hidden in:

- Any of the Status views (General, Job Activity and Statistics)
- Events Browser
- Reports
- Exported/archived event logs (you can remove anonymization when importing the exported logs).

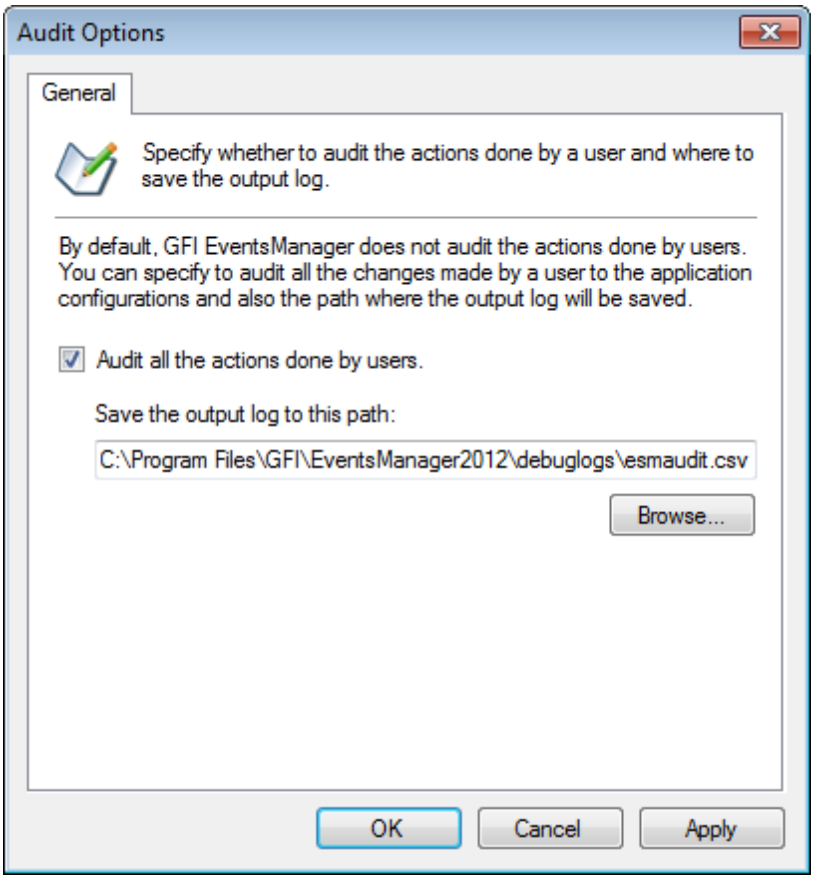
13.3 Auditing console activity

GFI EventsManager can save console activity to external logs. To configure console activity auditing:



Screenshot 193: Enabling console user activity auditing

1. From **Configuration** tab > **Options**, expand **Console Security and Audit Options** node.
2. Right-click **Audit Options** and select **Edit audit options...**.


Audit Options
General
Specify whether to audit the actions done by a user and where to save the output log.
By default, GFI EventsManager does not audit the actions done by users. You can specify to audit all the changes made by a user to the application configurations and also the path where the output log will be saved.
Audit all the actions done by users.
Save the output log to this path:
C:\Program Files\GFI\EventsManager2012\debuglogs\esmaudit.csv
Browse...
OK
Cancel
Apply

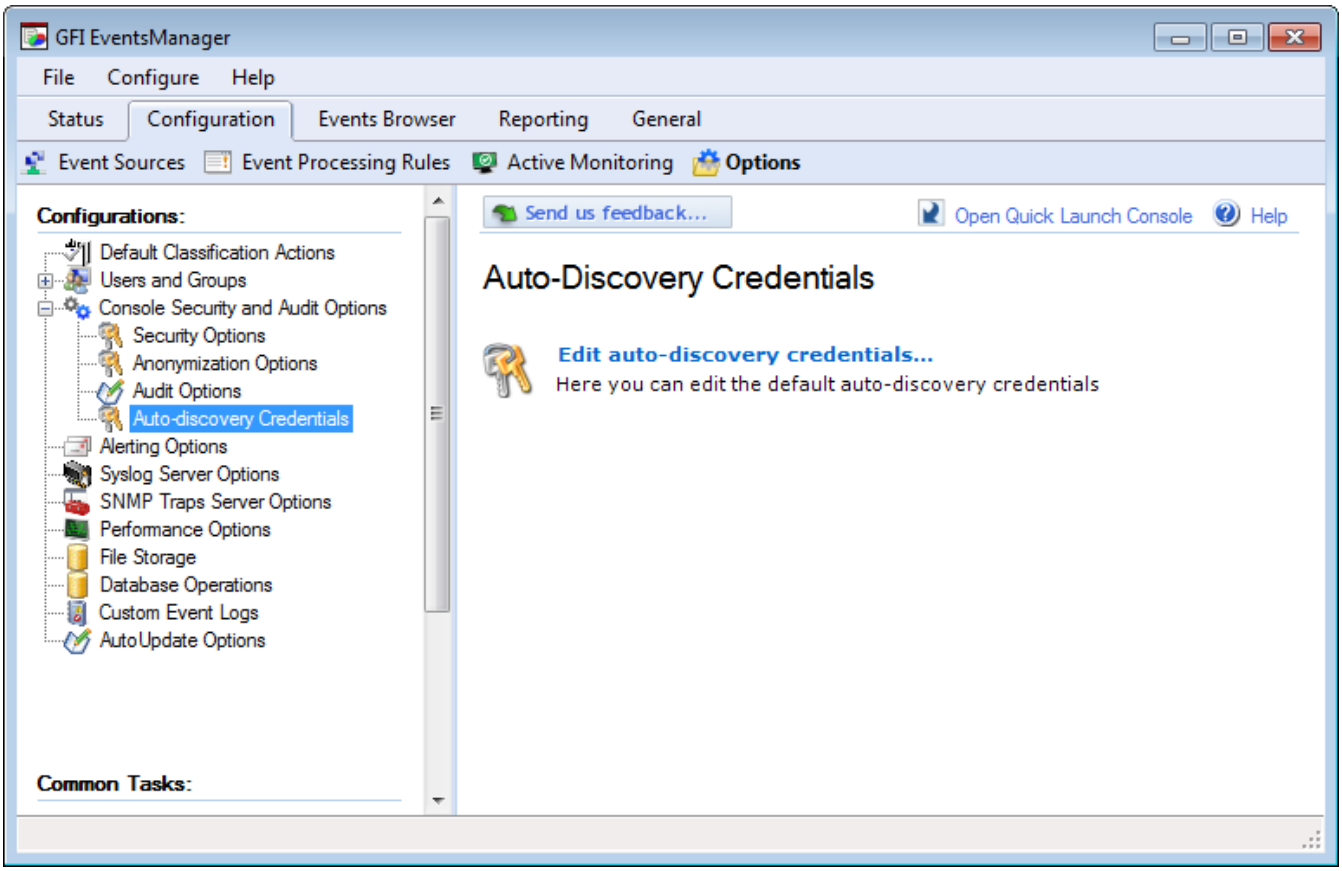
Screenshot 194: Audit Options dialog

3. Select **Audit all the actions done by users** option and specify the location where the output log file will be saved.

4. Click **Apply** and **OK**.

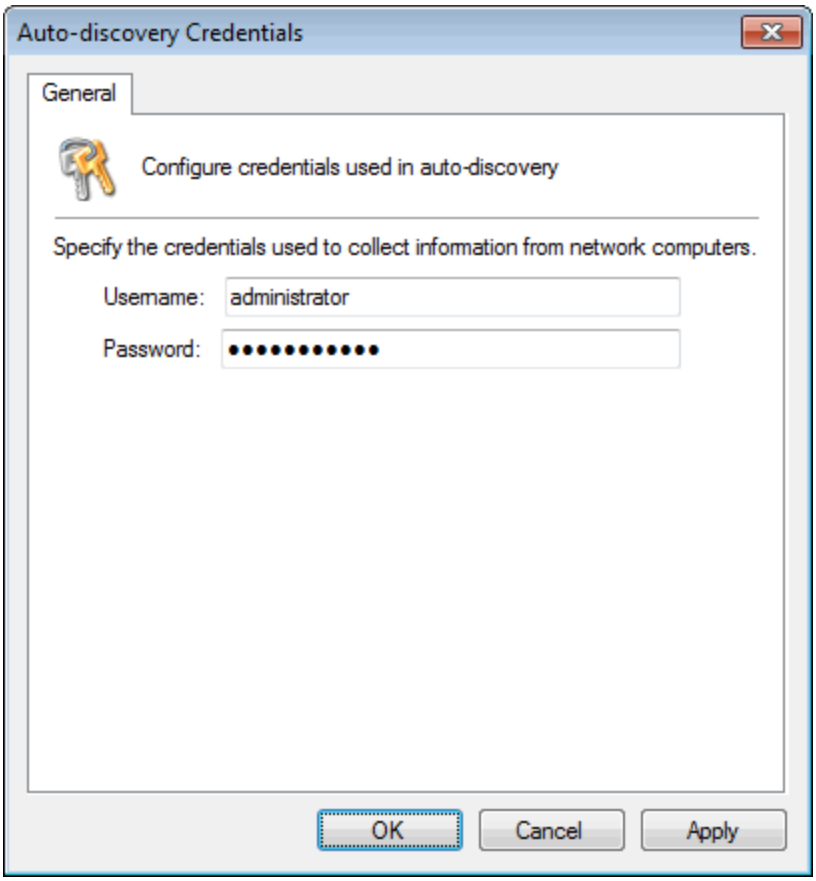
13.4 Auto-discovery credentials

Auto-discovery credentials are used by GFI EventsManager to login target machines and collect information when performing an automatic search for event sources. To configure the auto-discovery credentials:



Screenshot 195: Configuring Auto-Discovery Credentials

1. From **Configuration** tab > **Options**, expand **Console Security and Audit Options** node.
2. Right-click **Auto-discovery credentials** and select **Edit auto-discovery credentials**.



Screenshot 196: Specify Auto-discovery credentials

3. Key in a valid username and password.

4. Click **Apply** and **OK**.

14 Database Maintenance

This chapter provides information about the storage system that GFI EventsManager uses to store processed events. This system allows great scalability with its fast read/write capabilities; even when processing high volumes of data. To help you maintain your database backend, GFI EventsManager provides you with dedicated maintenance job options.

Database maintenance jobs provide advanced functionality to administrators, allowing them to:

- Centralize events collected by other remote GFI EventsManager instances into one database back-end
- Optimize GFI EventsManager performance by actively controlling database backend growth hence keeping it in good shape
- Import and export data to and from older versions of GFI EventsManager without data inconsistencies.
- Import and export events to and from a storage folder minimizing data loads from the database.

Topics in this chapter:

14.1 Managing the database backend 242

14.2 Creating maintenance jobs 252

14.3 Editing maintenance jobs 281

14.1 Managing the database backend

This section describes how you can easily manage your backend database through GFI EventsManager Management Console.

This section contains information about:

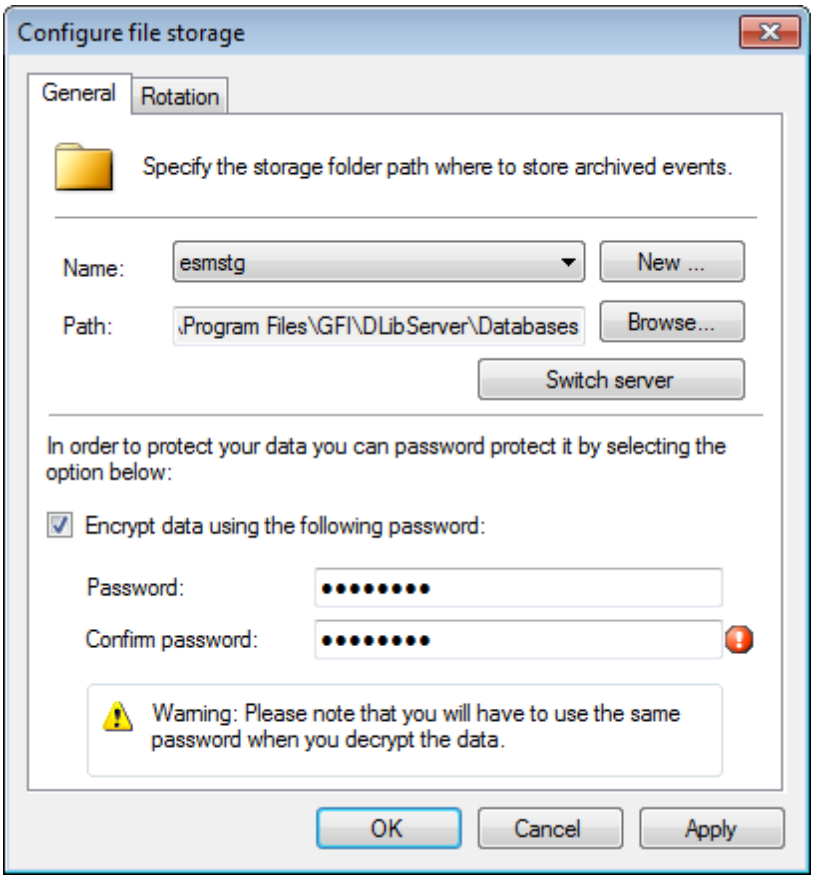
- Creating a new database
- Protecting your database
- Enabling database record hashing
- Switching databases
- Configuring database rotation options

14.1.1 Creating a new database

GFI EventsManager enables you to have multiple databases to store processed event logs. Through the Events Browser, Reporting tab and other locations, you can easily switch from one database to another, allowing you to view events or generate reports from multiple databases. Databases can be further secured by encrypting them with a password.

To create a new database:

1. From **Configuration** tab > **Options** > **Configurations**, right-click **File Storage** and select **Configure file storage**….



Screenshot 197: File storage system dialog

2. Click **New** and key in the new database name. Click **OK** to close the Create new database dialog.

3. Click **Browse** to select a location other than the default database store.

4. (Optional) Select **Encrypt data using the following password** and specify the encryption password used to secure information in the new database.

Note

Indicates that the specified passwords do not match.

5. Click **Apply** and **OK**.

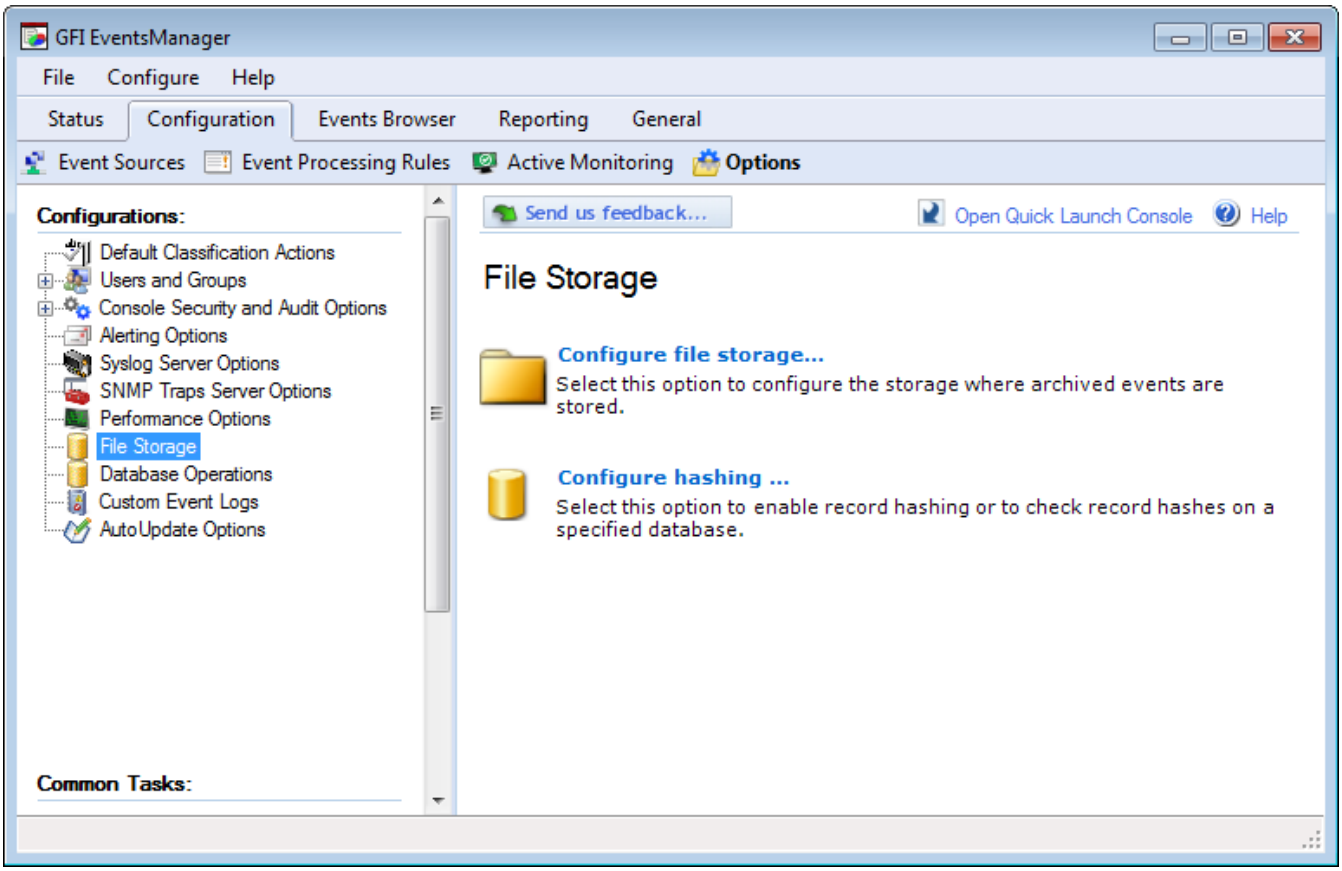
14.1.2 Protecting your database

GFI EventsManager enables you protect your database with an encryption key. Encrypting the database will prevent unauthorized personnel from viewing or accessing event logs.

Important

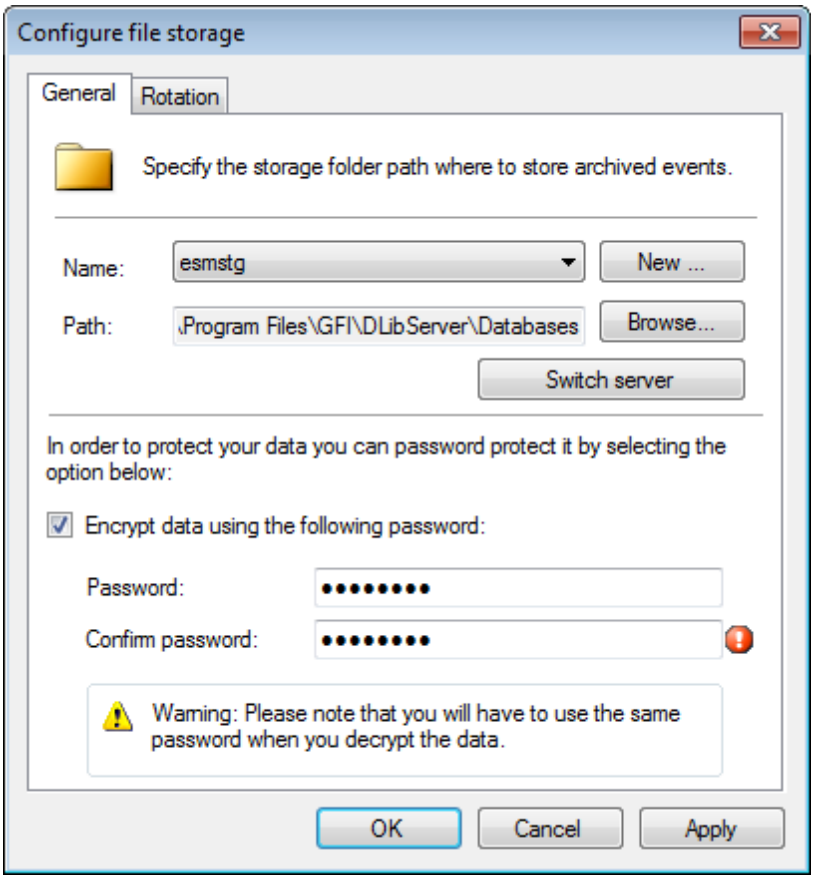
Encrypting the database will cause the **Status Monitor** and **Events Browser** to stop viewing sensitive information.

To encrypt the database backend:



Screenshot 198: Editing file storage settings

1. Click **Configuration** tab > **Options**, right-click **File Storage** and select **Configure file storage...**.



Screenshot 199: Enabling encryption

2. From **General** tab, select **Encrypt data using the following password** to enable encryption.

3. Specify the password and confirmation password.

> **Note**
>
> Indicates that the specified passwords do not match.

4. Click **Apply** and **OK**.

> **Note**
>
> The live database (the database you are currently using) cannot be encrypted from this dialog. Only new or offline databases can be encrypted from here. To encrypt the live database, use the provided CMD tool: **esmdlibm.exe**. For more information refer to Using Esmdlibm.exe.

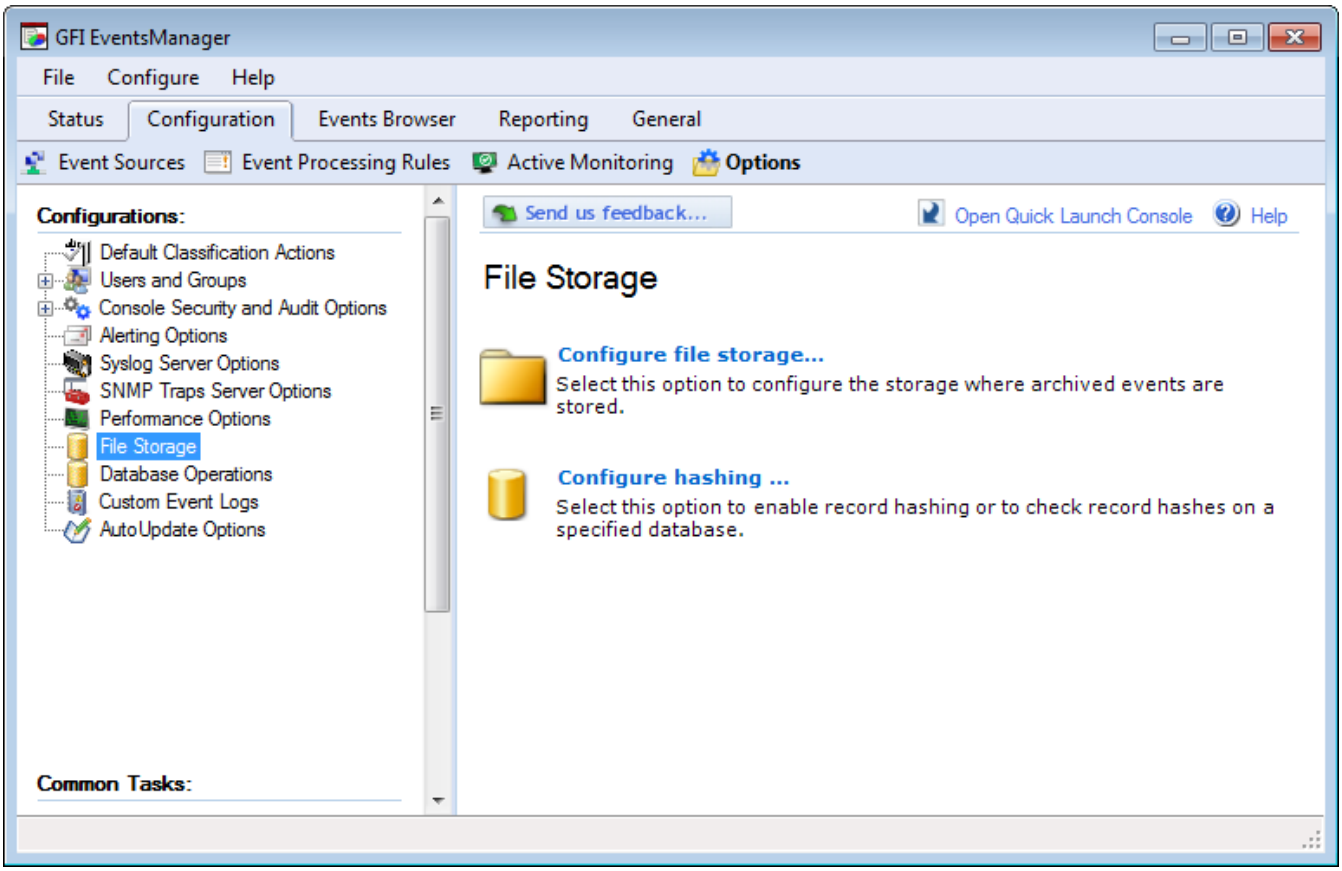
14.1.3 Database record hashing

To further protect your data, GFI EventsManager provides you with record hashing capabilities. Hashing new records is a method used to ensure that data in your databases remains unmodified. When record hashing is enabled, a hash is created for every collected log, at collection time. The hash is built based on the data contained in the event log itself and created as soon as the event log is collected to ensure that it is the original version. When data of a hashed record is modified (even a

character from a word), the hash value changes, indicating that someone could be tampering with stored records.

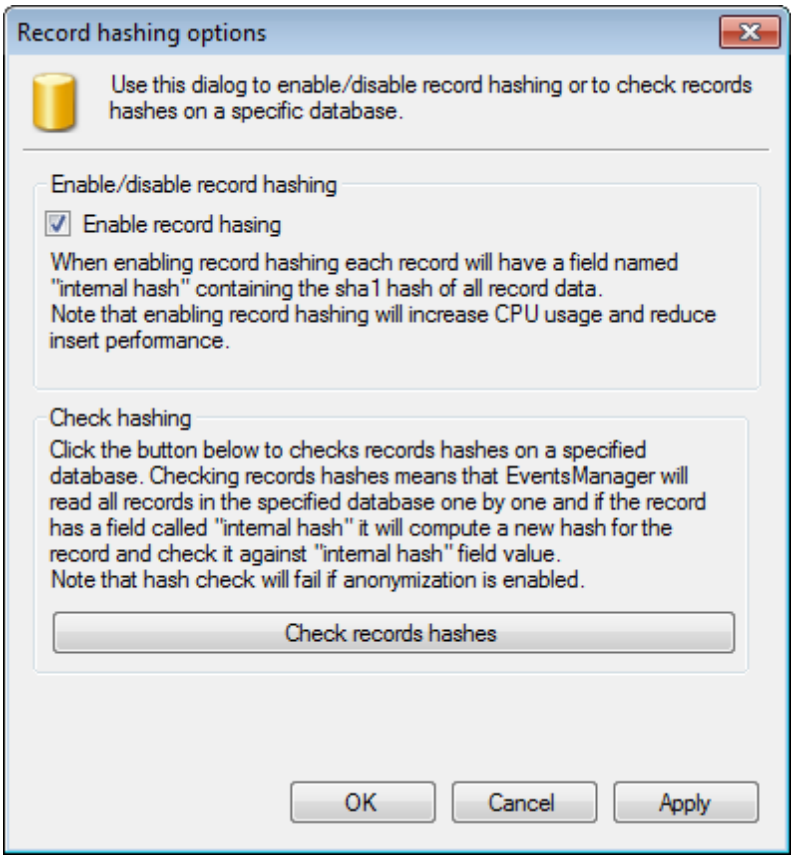
> **Important**
>
> Hashing will fail if anonymization is enabled.

To configure hashing:



Screenshot 200: Enabling / disabling record hashing

1. From **Configuration** tab **> Options > Configurations**, click **File Storage > Configure hashing...**.


Record hashing options
Use this dialog to enable/disable record hashing or to check records hashes on a specific database.
Enable/disable record hashing
Enable record hasing
When enabling record hashing each record will have a field named "internal hash" containing the sha1 hash of all record data.
Note that enabling record hashing will increase CPU usage and reduce insert performance.
Check hashing
Click the button below to checks records hashes on a specified database. Checking records hashes means that EventsManager will read all records in the specified database one by one and if the record has a field called "internal hash" it will compute a new hash for the record and check it against "internal hash" field value.
Note that hash check will fail if anonymization is enabled.
Check records hashes
OK
Cancel
Apply

Screenshot 201: Record hashing dialog

2. Select/unselect **Enable record hashing** to turn on/off hashing features.

3. Click **Check records hashes** to run hash checks on the selected database. Select a database from the list and click **OK** to start the check.

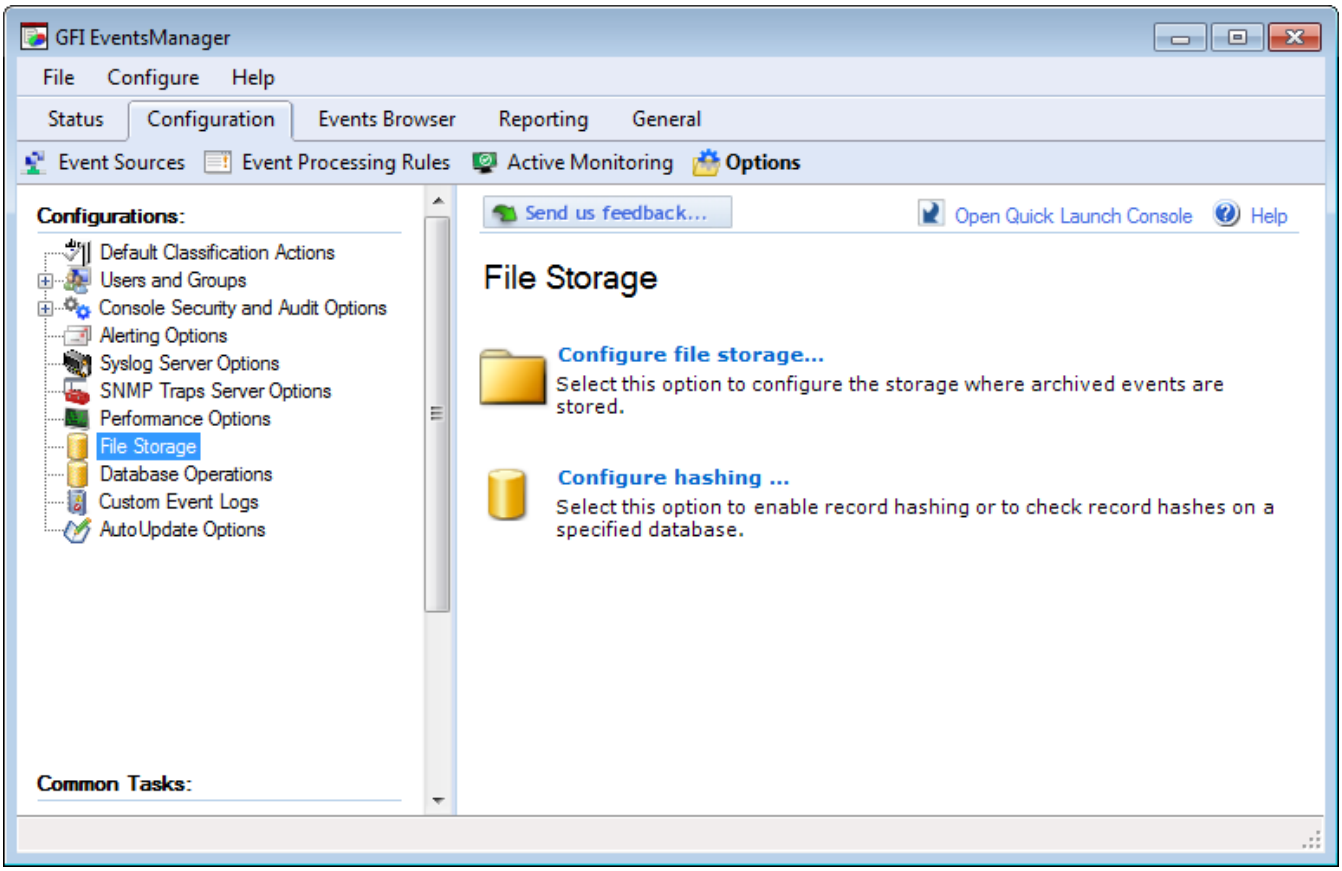
4. Click **Apply** and **OK**.

14.1.4 Switching between file storage databases

GFI EventsManager enables you to use multiple databases, stored in different locations on the same computer or on any remote computer within your LAN.

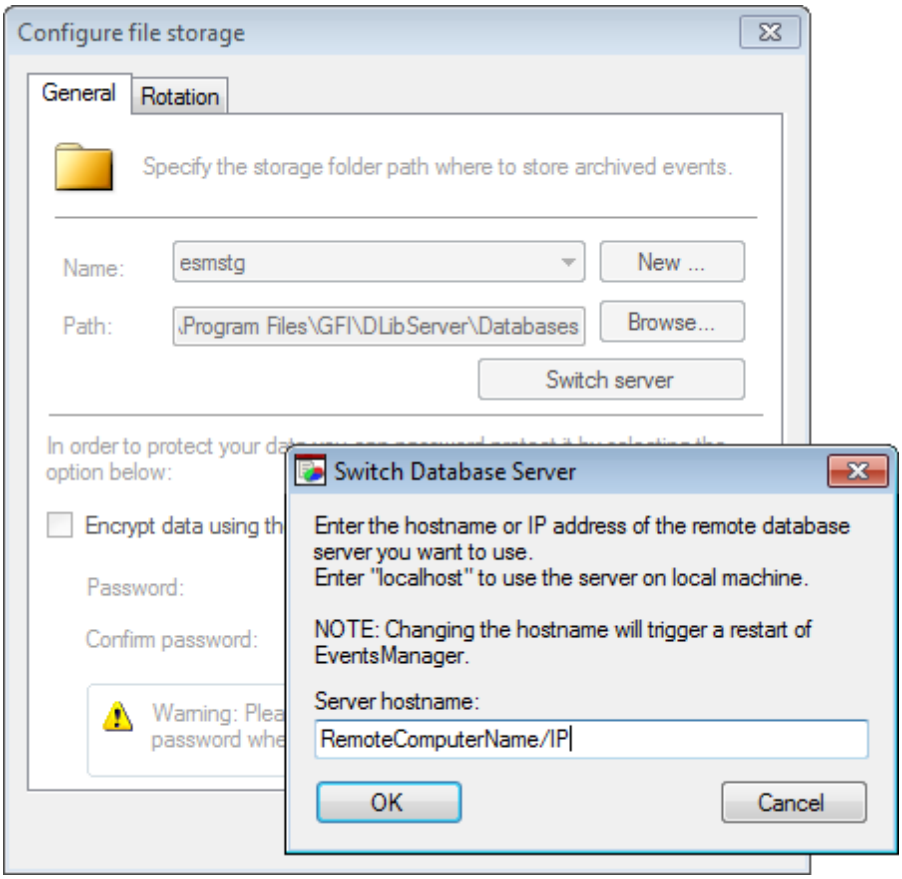
To switch between databases:

1. Click **Configuration** tab **> Options**.



Screenshot 202: Options tab

2. From the left pane, right-click **File Storage** and select **Configure file storage...**



3. From the Configure file storage dialog, click **Switch server**. This opens the Switch Database Server dialog.

4. In the **Server hostname** text box, key in the **Computer Name** or **IP address** of the database machine. Click **OK**.

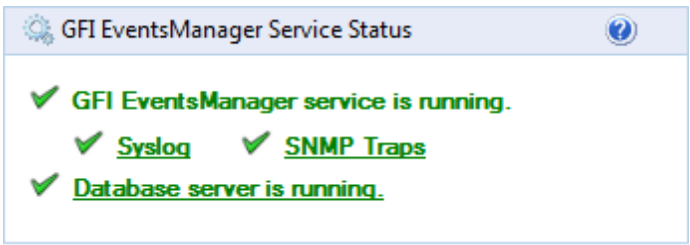
5. Click **Apply** and **OK**.

Switching databases from the dashboard

The General dashboard view enables you to switch to a different database without having to access the configuration tab. This is useful when comparing event logs or assessing the overall status of events management within your environment.

To switch to a different database from the dashboard:

1. Click **Status > General**.



Screenshot 203: Switch between databases from the dashboard

2. From the **GFI EventsManager Service Status** section, click **Database server is running**.

3. From the Configure file storage dialog, click **Switch server** and key in the database server **Name** or **IP** address. Click **OK**.

4. Click **Apply** and **OK**.

14.1.5 Configuring database rotation options

When processing events from a large number of event sources, it is important to configure database rotation options. These options instruct GFI EventsManager to automatically switch to a new database when a certain condition is met. Doing so helps you maintain a pool of fixed size databases which enable GFI EventsManager to perform better.

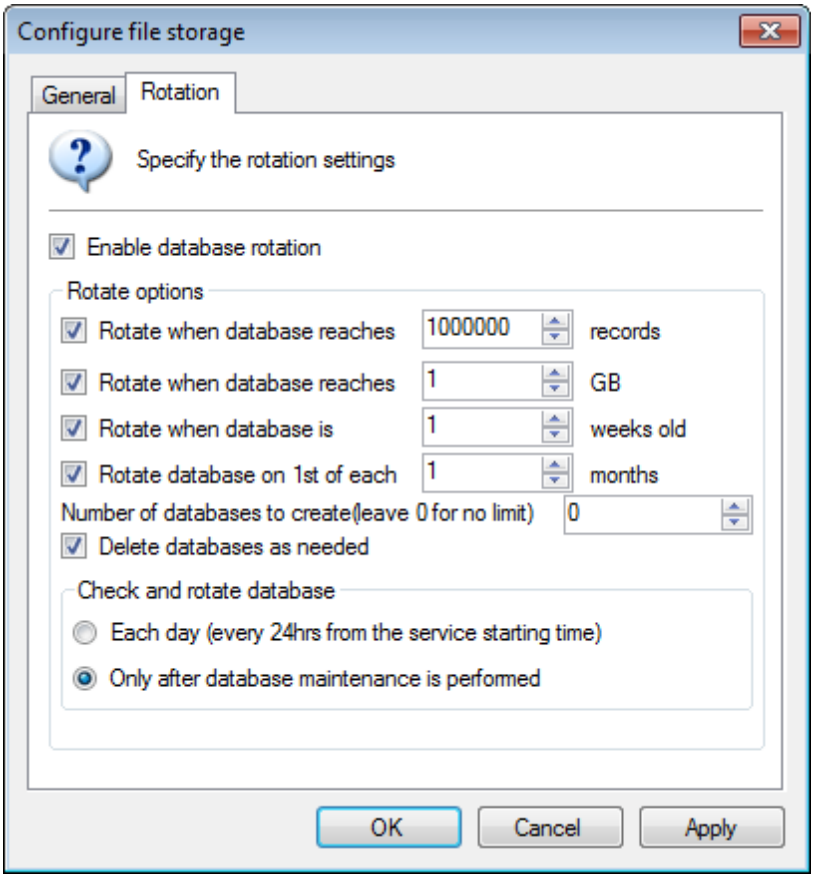
When a database becomes too large in size, queries take longer to complete so therefore, GFI EventsManager performance is affected negatively.

For example, if your event sources normally generate a lot of small sized event logs, enable database rotation for when a maximum number of records is reached. On the other hand, if the size of event logs that your event sources are generating is large, configure database rotation for when the database reaches the size limit.

To configure database rotation options:

1. Click **Configuration** tab **> Options**.

2. From **Configurations**, click **File storage > Configure file storage…**



Screenshot 204: Configuring database rotation options

3. Click **Enable database rotation**.

4. Configure the options described below:

Table 80: Database rotation options

Option	Description
Rotate when database reaches {X} Records	Specify the number of records that the database has to contain before rotating to a new one. **Note** Minimum value = 1,000, 000 records.
Rotate when database reaches {X} GB	Rotate to a new database when the current one reaches the specified size in Giga Bytes (GB) **Note** Minimum value = 1GB.
Rotate when database is {X} weeks old	Rotate database when the current one is older than the specified number of weeks. **Note** Minimum value = 1 week.
Rotate database on 1st of each {X} months	Select this option to rotate databases on the 1st of each number of specified months. Example, rotate database on the 1st of every month, 1st of every two months or 1st of every six months.
Number of databases to create	Specify the maximum number of databases that GFI EventsManager is able to create. Leave the value at **0** so that an unlimited number of databases can be created.
Delete database as needed	Select this option so that when the maximum number of databases is reached, GFI EventsManager automatically deletes the oldest database to free space for new ones.
Each day (every 24hrs from the service starting time)	Select this option to create and use a new database every 24 hours. 24 hours are calculated from the time the GFI EventsManager service starts.
Only after database maintenance is performed	Create and use a new database, after an existing database performs maintenance operations.

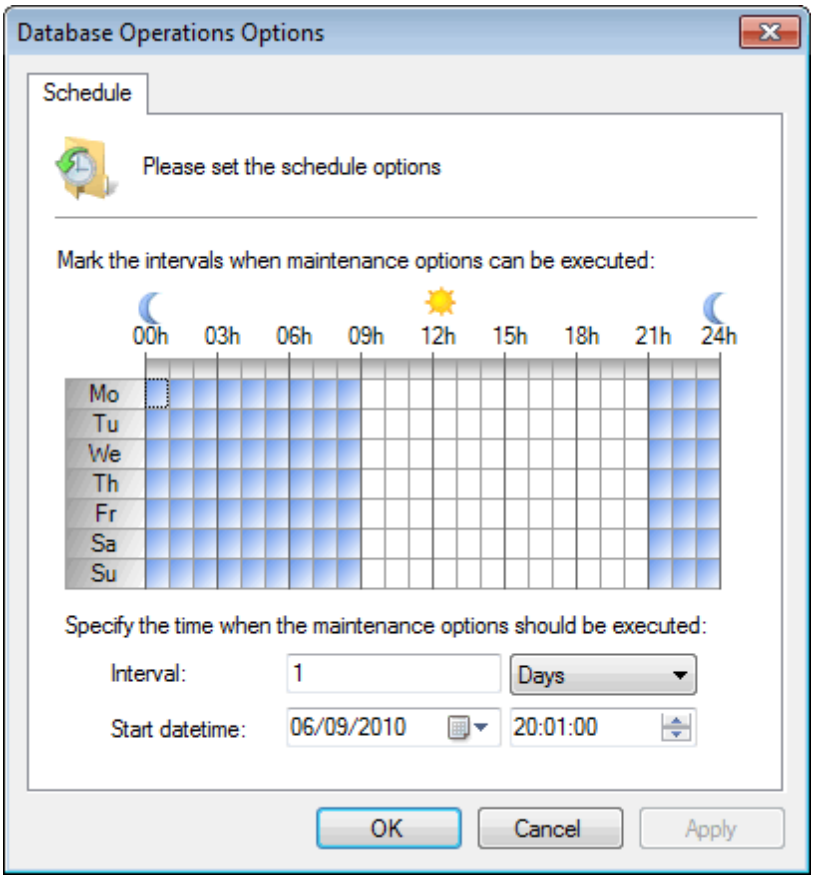
5. Click **Apply** and **OK**.

14.1.6 Configuring Database Operations

To configure Database Operations:

1. Click **Configuration** tab **> Options**.

2. From **Configurations**, right-click **Database Operations** and select **Properties**.



Screenshot 205: Database Operations Options dialog

3. Configure the options from the tabs described below:

Table 81: Configuring database operations

Tab	Description
General	Specify the unique identifier by which this instance of GFI EventsManager will be identified on the network. This identifier is used as part of the export file-name during Export to file operations.
Schedule	Through the Schedule tab, specify: » Hours of the day during which maintenance jobs can be executed » The interval in hours/days with which maintenance jobs will be executed » The scheduled date/time when maintenance jobs will start being executed.

4. Click **Apply** and **OK**.

> **Note**
>
> Schedule options can also be modified from **Configuration** tab > **Options** > **Actions** and click **Edit schedule options...**.

14.2 Creating maintenance jobs

With GFI EventsManager you can schedule maintenance jobs to be executed on a specific day, at a specific time and at specific intervals. Database maintenance operations may require high utilization of resources. This can degrade server and GFI EventsManager performance. Schedule maintenance jobs to be executed after office hours to maximize the availability of your system resources and avoid any possible disruptions to workflow.

GFI EventsManager supports two types of maintenance jobs as described below:

Table 82: Maintenance jobs types

Job type	Description
Import\Export Job	Import/export data from/to other instances of GFI EventsManager. Export data and import them in other instances as part of the data centralization process.
Legacy Import Job	Import data from older versions of the product. Import data from Microsoft® SQL Server® databases, legacy files and legacy file storage. The import jobs supported by this job type are all based on the database backend types of older versions of GFI EventsManager.

Read the following sections for information about creating the following maintenance jobs:

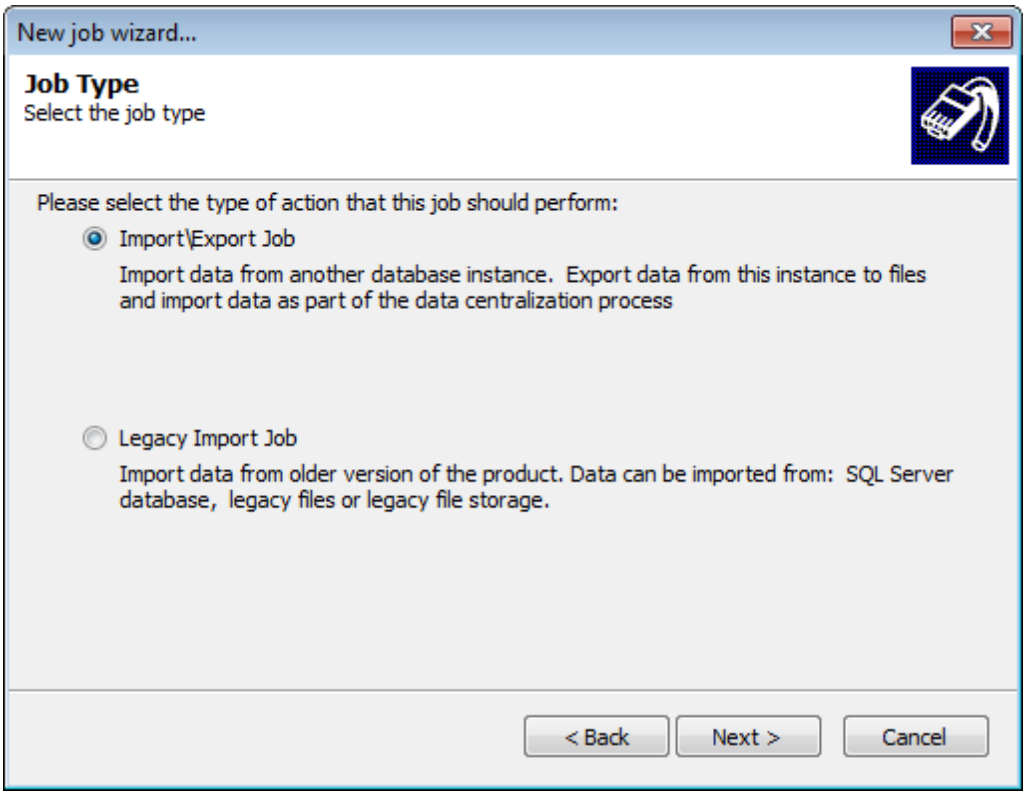
- Import from file
- Export to file
- Export to SQL
- Copy data
- Commit deletions
- Import from SQL Server® databases
- Import from legacy files
- Import from legacy file storage

14.2.1 Import from file

Import from file job enables you to import data that was previously exported to a configuration file.

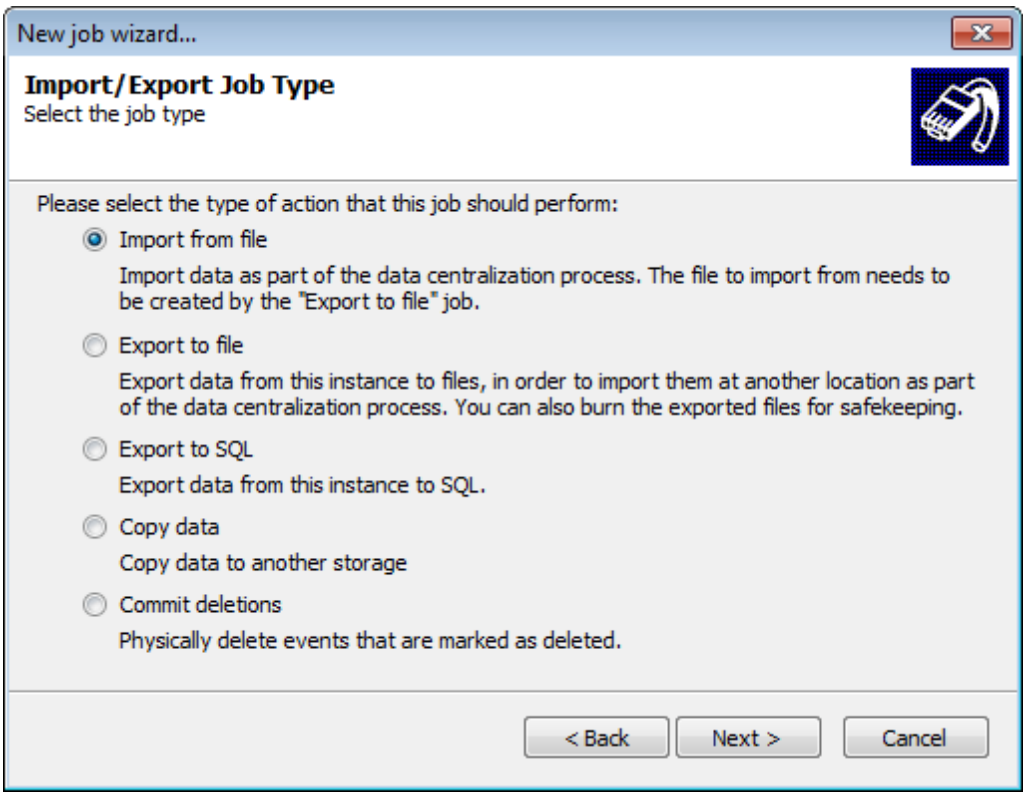
To create an Import from file job:

1. Click **Configuration** tab and select **Options**.
2. From **Configurations**, right-click **Database Operations** node and select **Create new job**…
3. Click **Next** at the wizard welcome screen.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

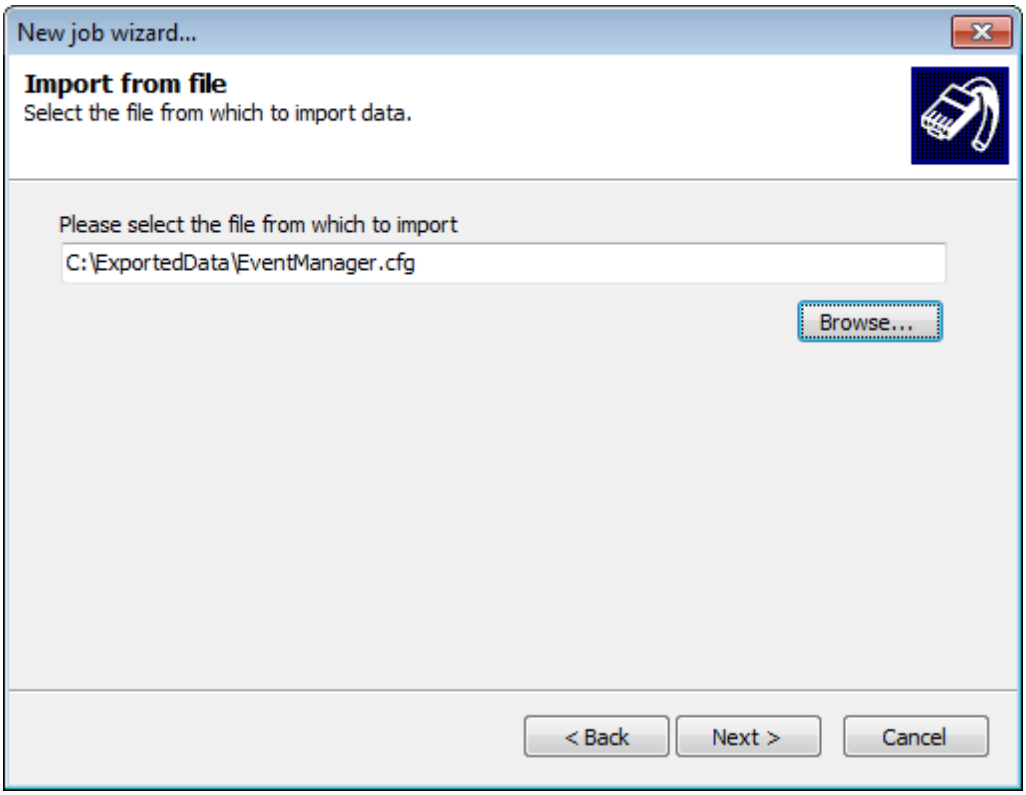
Screenshot 206: Creating Import\Export jobs

4. Select **Import/Export Job** and click **Next**.


New job wizard...
Import/Export Job Type
Select the job type
Please select the type of action that this job should perform:
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Export to SQL
Export data from this instance to SQL.
Copy data
Copy data to another storage
Commit deletions
Physically delete events that are marked as deleted.
< Back
Next >
Cancel

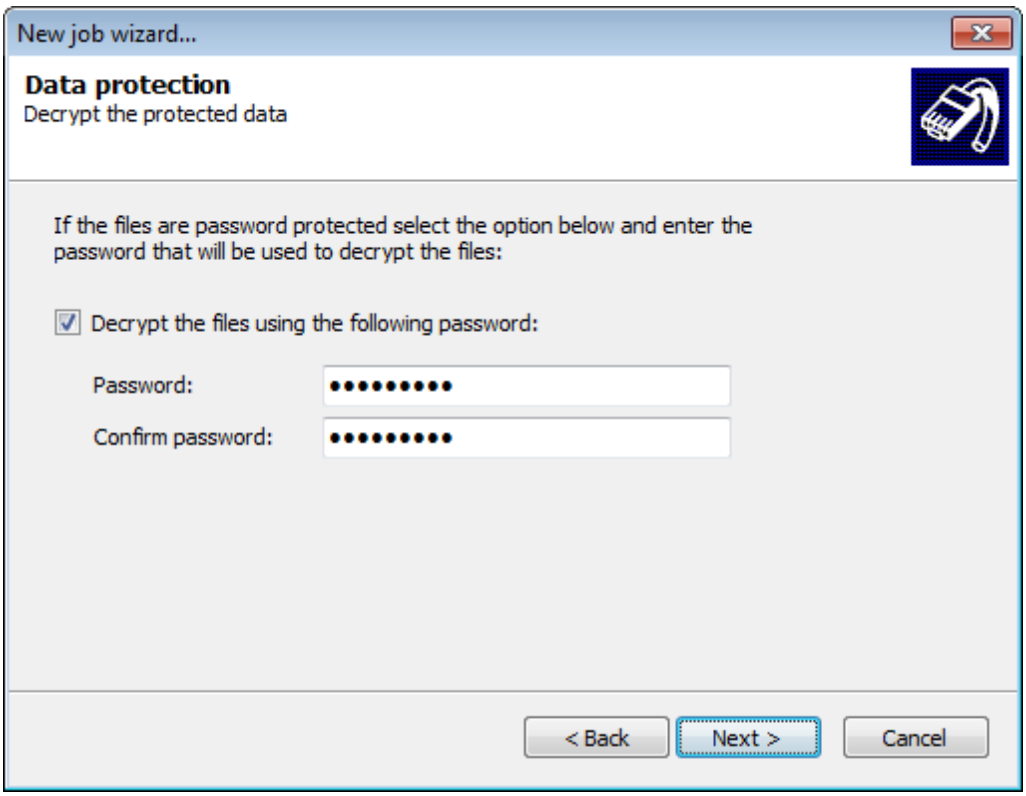
Screenshot 207: Import from file

5. Select **Import from file** and click **Next**.



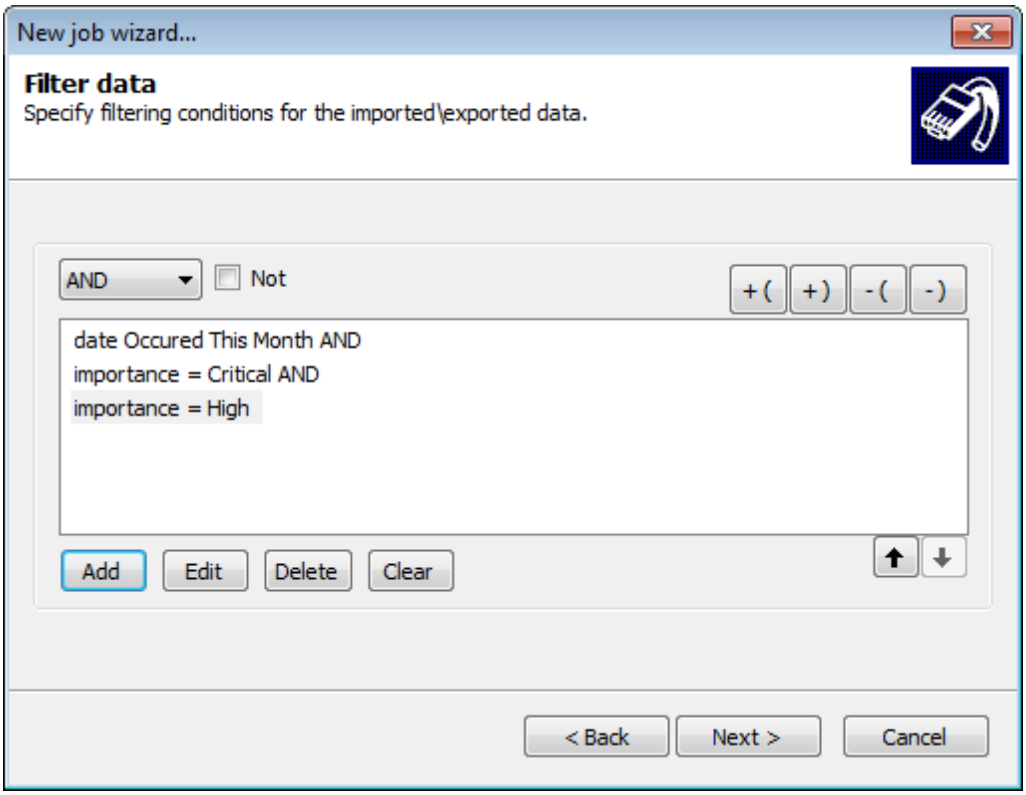
Screenshot 208: Import from file - Specify import file path

6. Specify the path to the configuration file that contains data you want to import. Optionally, click **Browse** to look for the location. Click **Next**.


New job wizard...
Data protection
Decrypt the protected data
If the files are password protected select the option below and enter the password that will be used to decrypt the files:
Decrypt the files using the following password:
Password:
Confirm password:
< Back
Next >
Cancel

Screenshot 209: Decrypt secure import files

7. (Optional) If the file you are importing is encrypted, select **Decrypt the files using the following password** and specify the password used to encrypt the file. Click **Next**.

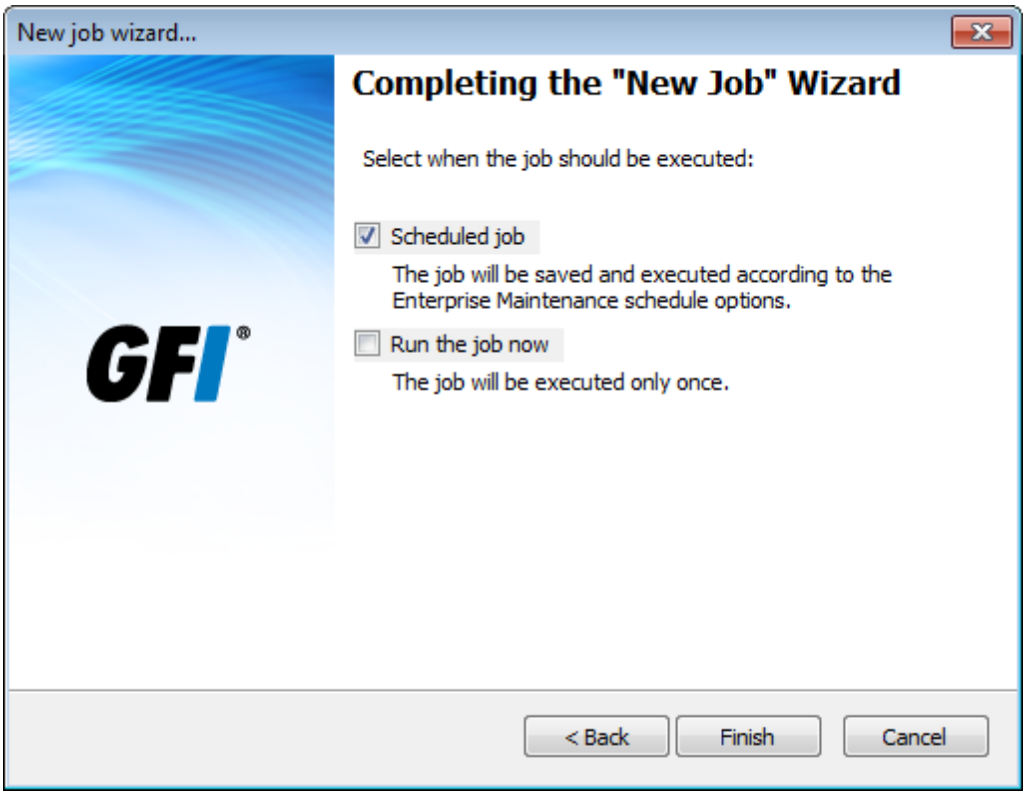


Screenshot 210: Add filtering conditions

8. Add advanced filtering parameters to import specific data only. Leave blank to import all the event logs from the file.

Note

For more information refer to Building Query Restrictions.


New job wizard...
Completing the "New Job" Wizard
Select when the job should be executed:
Scheduled job
The job will be saved and executed according to the Enterprise Maintenance schedule options.
Run the job now
The job will be executed only once.
< Back
Finish
Cancel

Screenshot 211: Execute job options

9. Select when the job is executed and click **Finish**:

Table 83: Creating maintenance jobs - Schedule options

Options	Description
Schedule job	The job will be saved and executed according to the database operations schedule.
Run the job now	Job is executed immediately. Unscheduled jobs only run once and cannot be reused.

14.2.2 Export to file

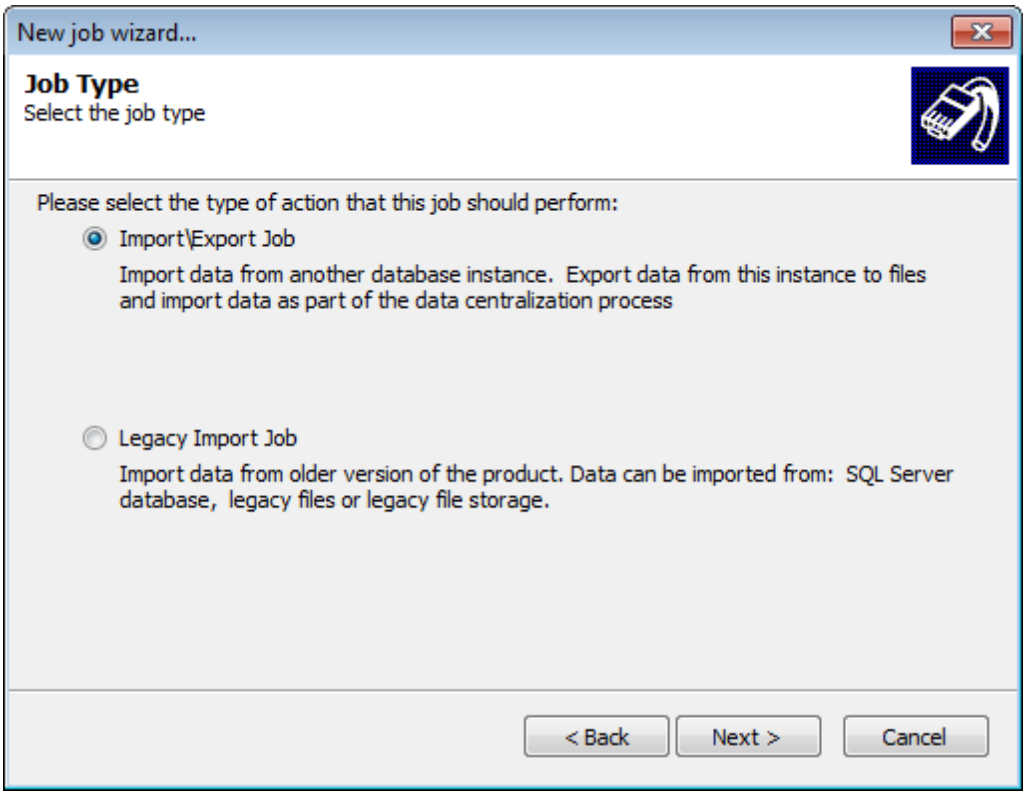
Export to file enables you to export selected settings to a configuration file that can be imported by another instance or version of GFI EventsManager.

To create an export to file job:

1. Click **Configuration** tab and select **Options**.

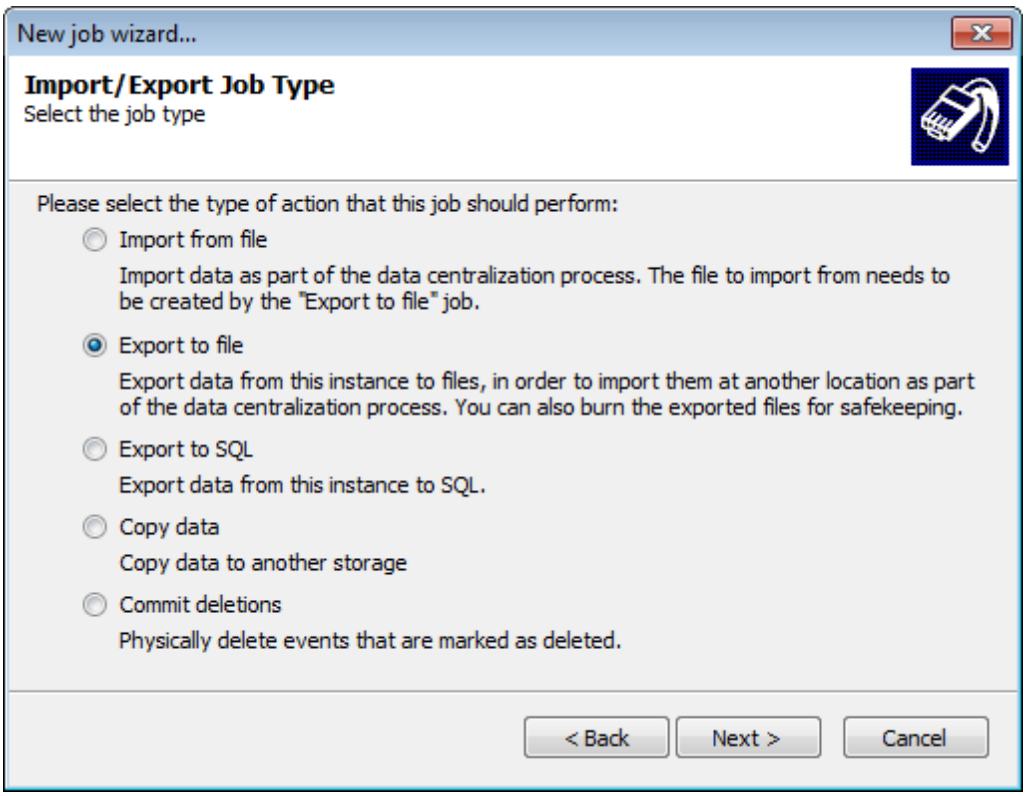
2. From **Configurations**, right-click **Database Operations** node and select **Create new job…**

3. Click **Next** at the wizard welcome screen.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

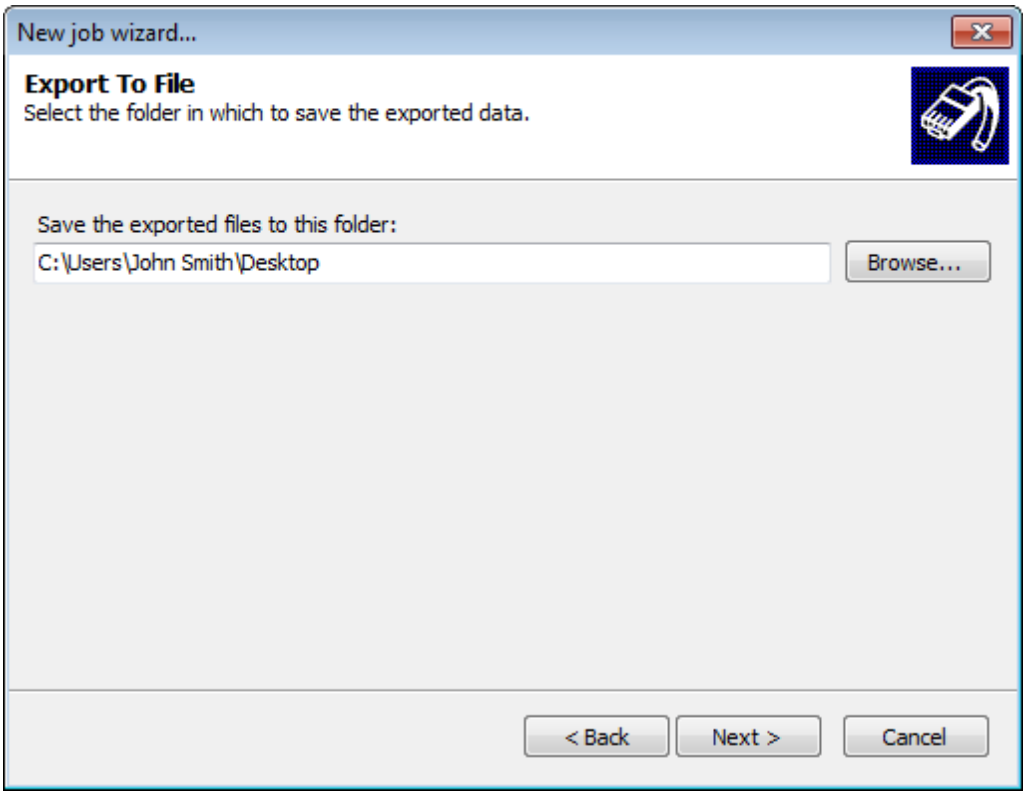
Screenshot 212: Creating Import\Export jobs

4. Select **Import/Export Job** and click **Next**.


New job wizard...
Import/Export Job Type
Select the job type
Please select the type of action that this job should perform:
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Export to SQL
Export data from this instance to SQL.
Copy data
Copy data to another storage
Commit deletions
Physically delete events that are marked as deleted.
< Back
Next >
Cancel

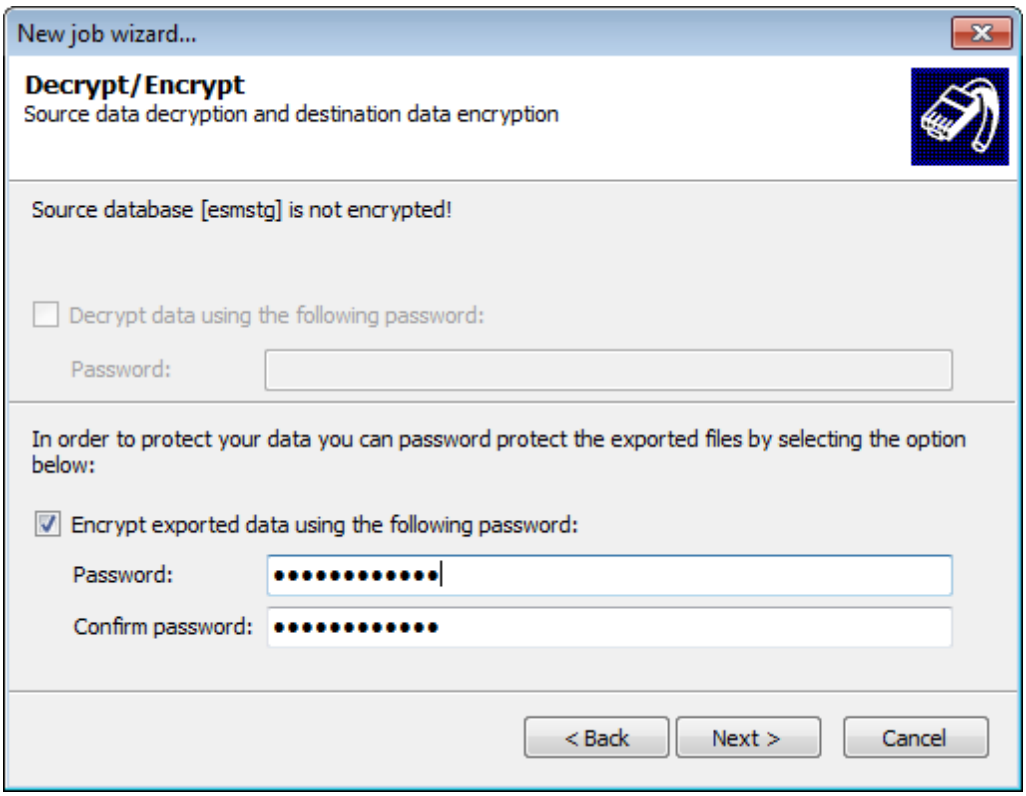
Screenshot 213: Export to file

5. Select **Export to file** and click **Next**.



Screenshot 214:

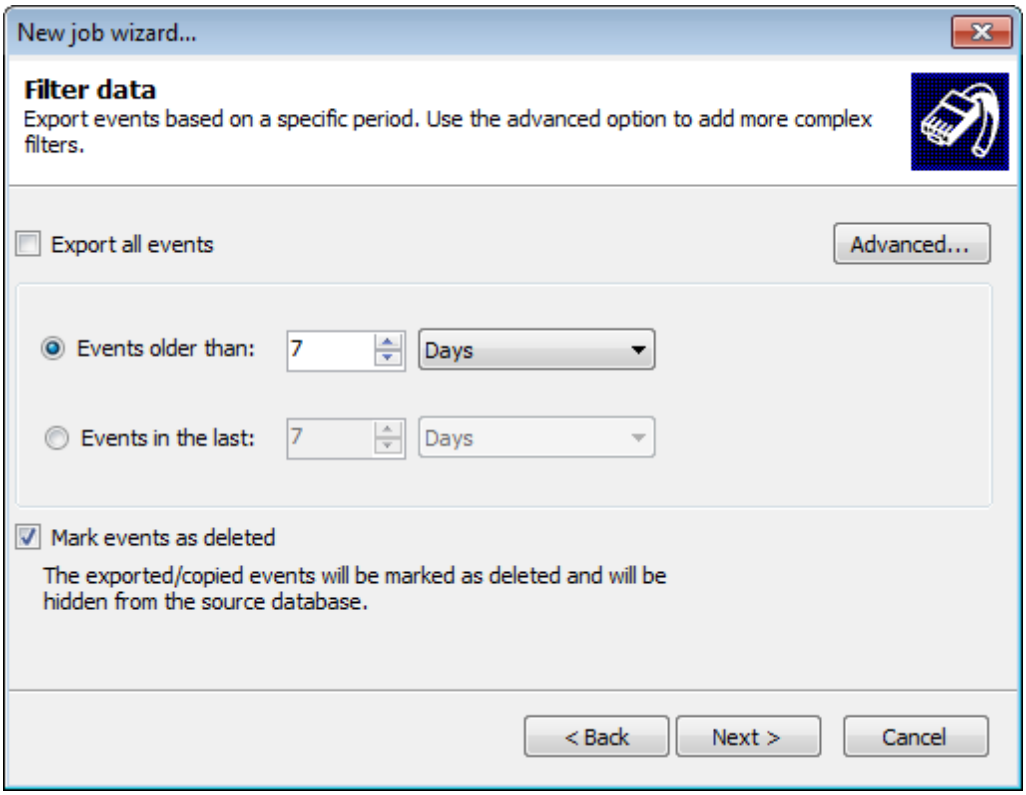
6. Key in the path to the folder where exported files are saved to. Alternatively, click **Browse** to look for the location. Click **Next**.


New job wizard...
Decrypt/Encrypt
Source data decryption and destination data encryption
Source database [esmstg] is not encrypted!
Decrypt data using the following password:
Password:
In order to protect your data you can password protect the exported files by selecting the option below:
Encrypt exported data using the following password:
Password:
Confirm password:
< Back
Next >
Cancel

Screenshot 215: Decrypt/Encrypt data

7. If the source database (esmstg) is encrypted, select **Decrypt data using the following password** and key in the decryption key in the **Password** field.

8. To encrypt export data, select **Encrypt exported data using the following password** and key in an encryption key in the **Password** and **Confirm password** fields. Click **Next**.

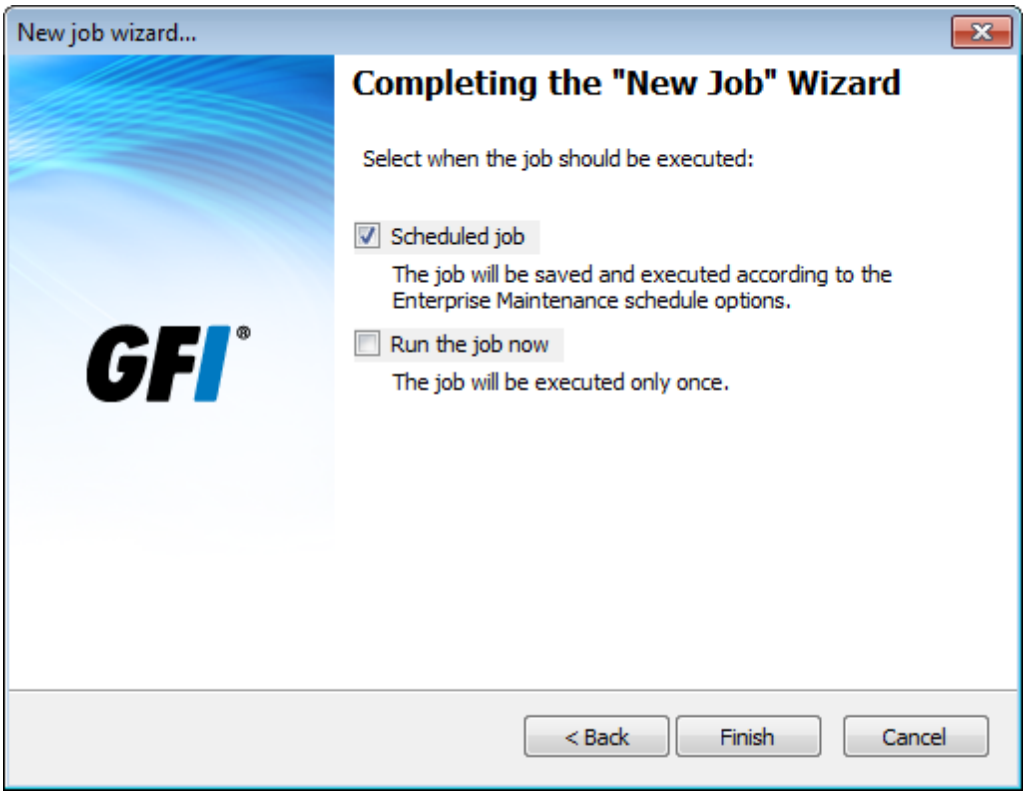

New job wizard...
Filter data
Export events based on a specific period. Use the advanced option to add more complex filters.
Export all events
Advanced...
Events older than:
7
Days
Events in the last:
7
Days
Mark events as deleted
The exported/copied events will be marked as deleted and will be hidden from the source database.
< Back
Next >
Cancel

Screenshot 216: Filtering export data

9. Configure the following filtering options and click **Next**:

Table 84: Filtering export data

Option	Description
Export all events	Export all events from the database.
Events older than	Only export events older than the specified number of days/weeks/months.
Events in the last	Only export events that occurred in the last specified number of days/weeks/months.
Mark events as deleted	Hide events from the source database after they are exported. To completely remove these events from the database, you must run a Commit Deletions job. For more information refer to Commit deletions.
Advanced...	Click **Advanced...** to launch the Advanced Filtering dialog. This enables you to configure granular filtering parameters to export specific events only. For more information refer to Building query restrictions.


New job wizard...
Completing the "New Job" Wizard
Select when the job should be executed:
Scheduled job
The job will be saved and executed according to the Enterprise Maintenance schedule options.
Run the job now
The job will be executed only once.
< Back
Finish
Cancel

Screenshot 217: Execute job options

10. Select when the job is executed and click **Finish**:

Table 85: Creating maintenance jobs - Schedule options

Options	Description
Schedule job	The job will be saved and executed according to the database operations schedule.
Run the job now	Job is executed immediately. Unscheduled jobs only run once and cannot be reused.

Export filename

The convention used by GFI EventsManager to name the export file is shown and described below:

```
[ESM ID]_[Job ID]_[Date From]_[Date To].EXP
```

Table 86: Database operations: Export file name structure

Name Section	Description
ESM ID	Refers to the unique identifier given to each GFI EventsManager instance running in the organization.
Job ID	Refers to the unique identifier given to each maintenance job created.
Date From	Refers to the date of the earliest event exported.
Date To	Refers to the date of the latest event exported.
.EXP	This is the file extension given to all export files.

14.2.3 Export to SQL

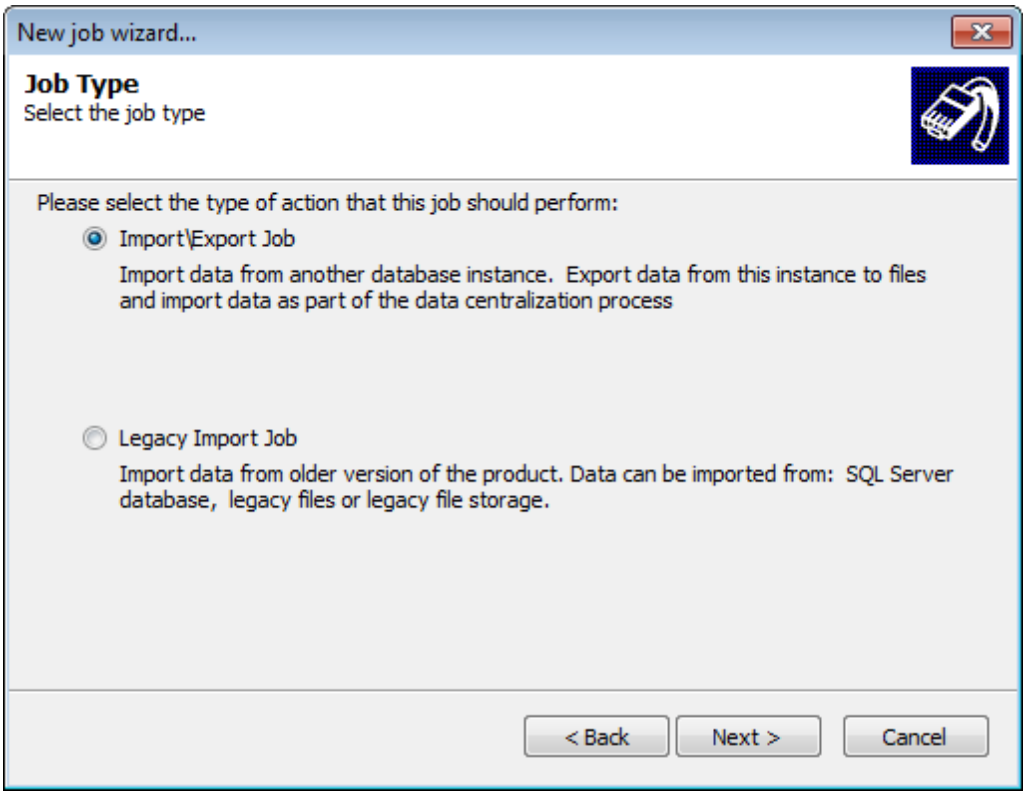
Export to SQL enables you to export items directly to an SQL Server instance that is reachable by the GFI EventsManager host.

To create an export to SQL job:

1. Click **Configuration** tab and select **Options**.

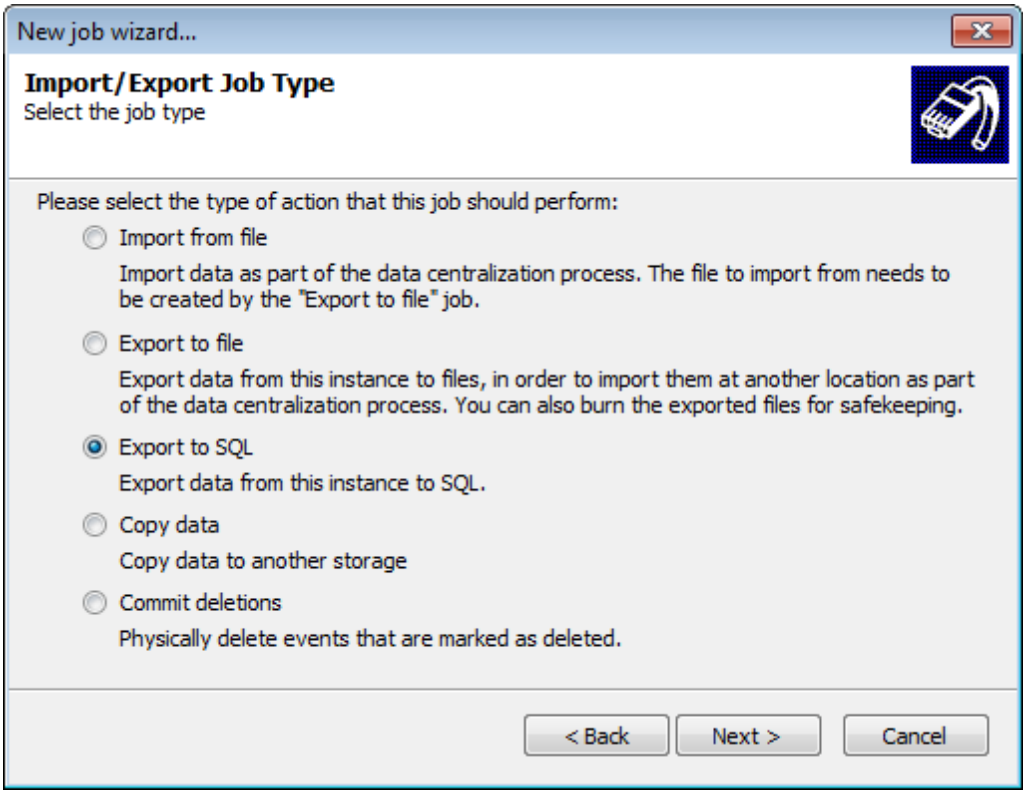
2. From **Configurations**, right-click **Database Operations** node and select **Create new job…**

3. Click **Next** at the wizard welcome screen.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

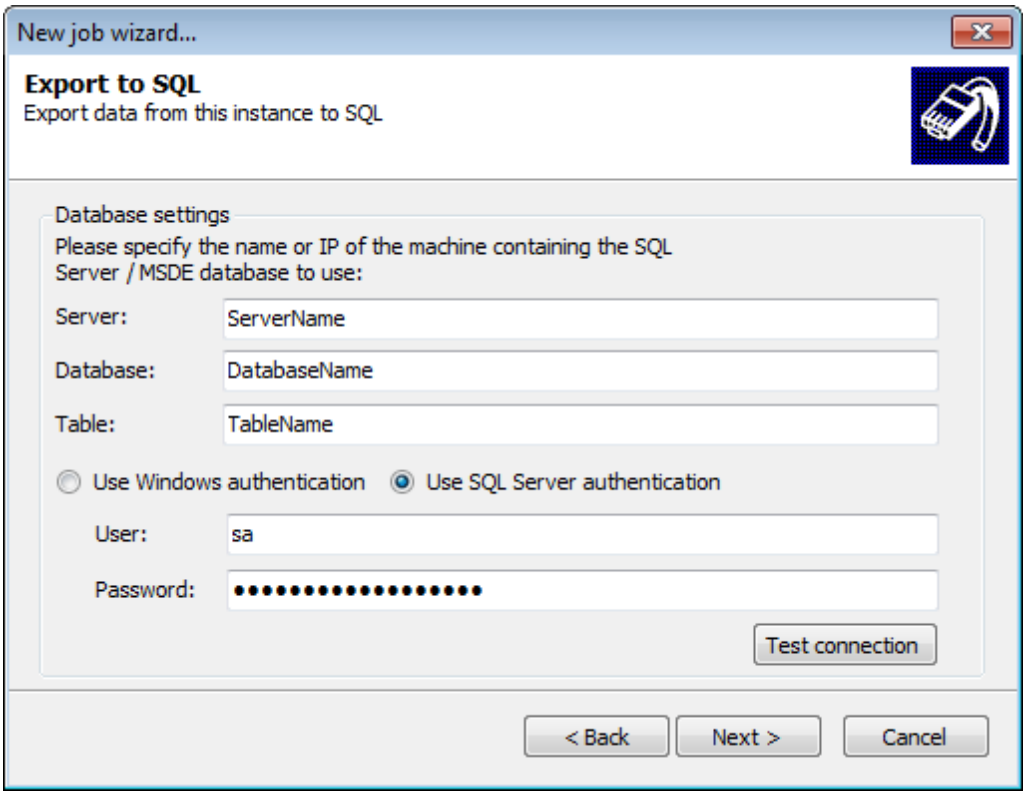
Screenshot 218: Creating Import\Export jobs

4. Select **Import/Export Job** and click **Next**.


New job wizard...
Import/Export Job Type
Select the job type
Please select the type of action that this job should perform:
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Export to SQL
Export data from this instance to SQL.
Copy data
Copy data to another storage
Commit deletions
Physically delete events that are marked as deleted.
< Back
Next >
Cancel

Screenshot 219: Export to SQL

5. Select **Export to SQL** and click **Next**.

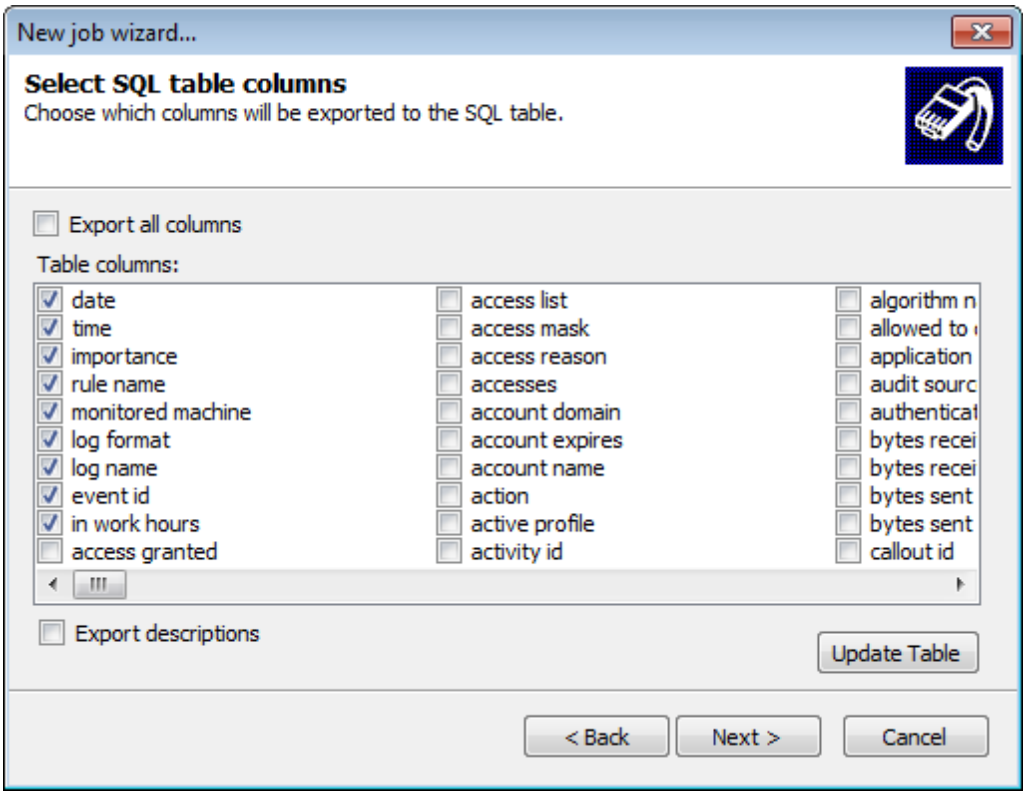


Screenshot 220: Specifying SQL Server details

6. Configure the following server options and click **Next**:

Table 87: Export to SQL - Server options

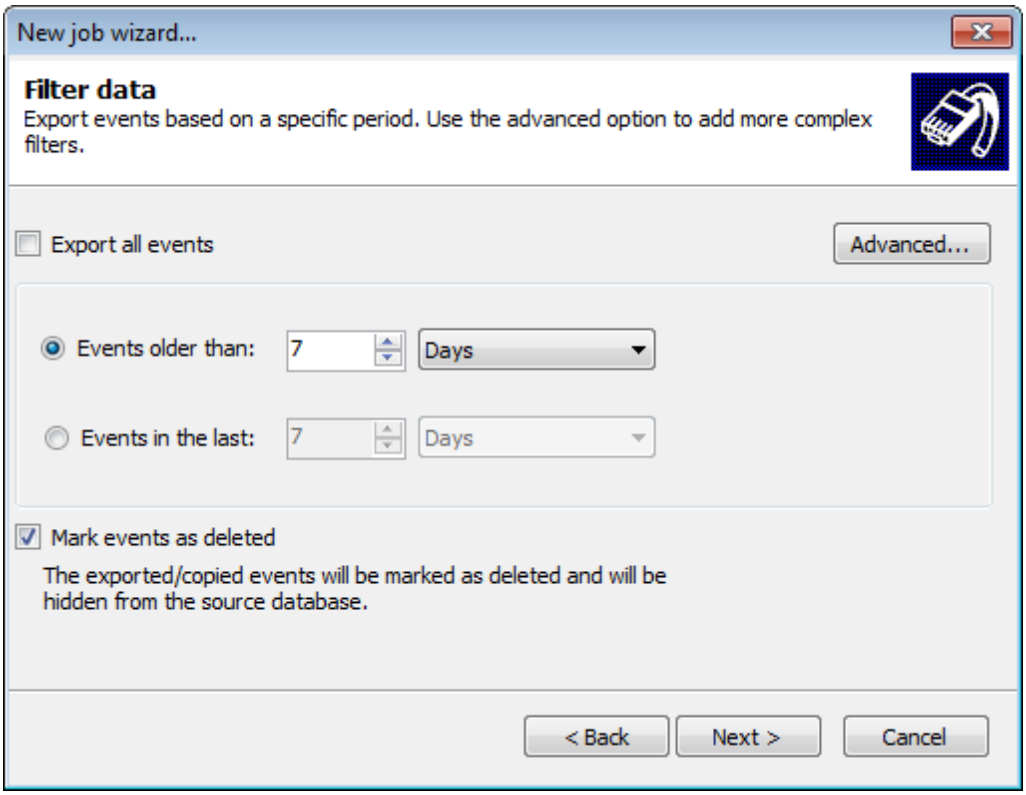
Option	Description
Server	Key in the name of the machine that is running SQL Server.
Database	Key in the name of the destination database. **Note** If the specified database does not exist, GFI EventsManager creates it for you.
Table	Key in the name of the destination table. **Note** If the specified table does not exist, GFI EventsManager creates it for you.
Use Windows authentication	Use the same logon credentials used to log on to Windows®. The SQL Server® must support this type of authentication mode to be able to connect and copy information to the server.
Use SQL Server authentication	Use the logon credentials configured in your SQL Server®. Key in the username in the **User** field and the password in the **Password** field.
Test connection	Click **Test Connection** to attempt to connect to the SQL Server® using the specified settings. **Note** GFI EventsManager tests the connection automatically after you click **Next**.



Screenshot 221: Select columns to export

7. Select the columns you want to export and click **Next**.

> **Note**
>
> To export all columns, select **Export all columns**.

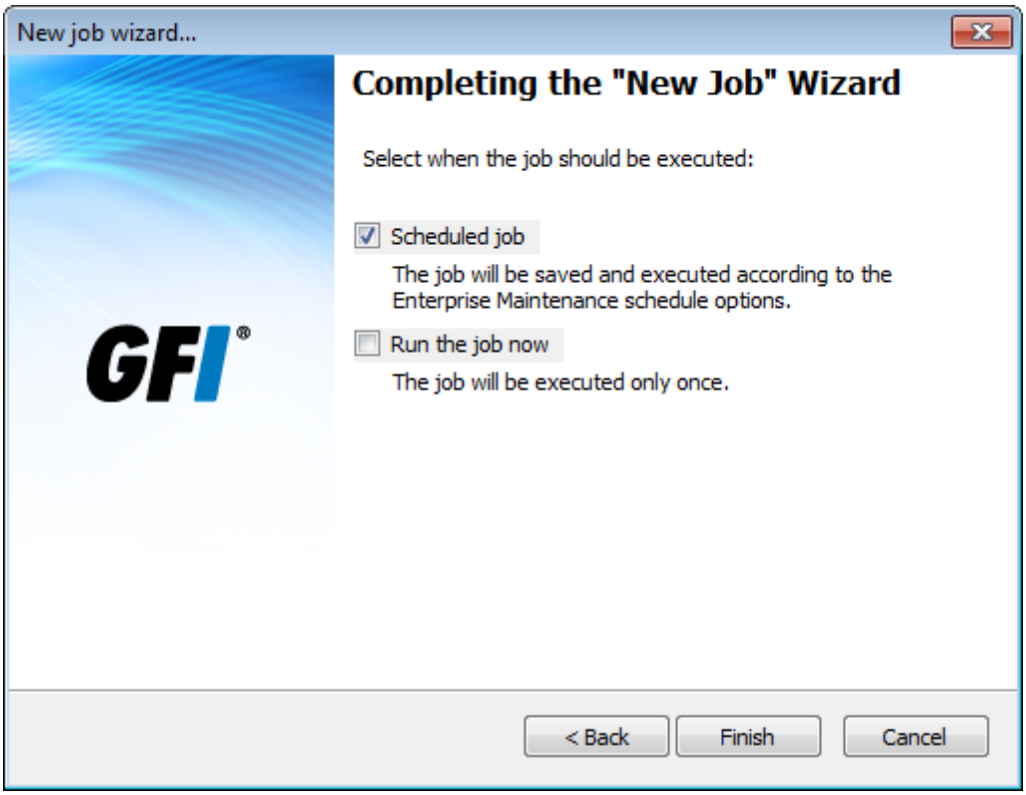

New job wizard...
Filter data
Export events based on a specific period. Use the advanced option to add more complex filters.
Export all events
Advanced...
Events older than:
7
Days
Events in the last:
7
Days
Mark events as deleted
The exported/copied events will be marked as deleted and will be hidden from the source database.
< Back
Next >
Cancel

Screenshot 222: Filtering export data

8. Configure the following filtering options and click **Next**:

Table 88: Filtering export data

Option	Description
Export all events	Export all events from the database.
Events older than	Only export events older than the specified number of days/weeks/months.
Events in the last	Only export events that occurred in the last specified number of days/weeks/months.
Mark events as deleted	Hide events from the source database after they are exported. To completely remove these events from the database, you must run a Commit Deletions job. For more information refer to Commit deletions.
Advanced...	Click Advanced... to launch the Advanced Filtering dialog. This enables you to configure granular filtering parameters to export specific events only. For more information refer to Building query restrictions.


New job wizard...
Completing the "New Job" Wizard
Select when the job should be executed:
Scheduled job
The job will be saved and executed according to the Enterprise Maintenance schedule options.
Run the job now
The job will be executed only once.
< Back
Finish
Cancel

Screenshot 223: Execute job options

9. Select when the job is executed and click **Finish**:

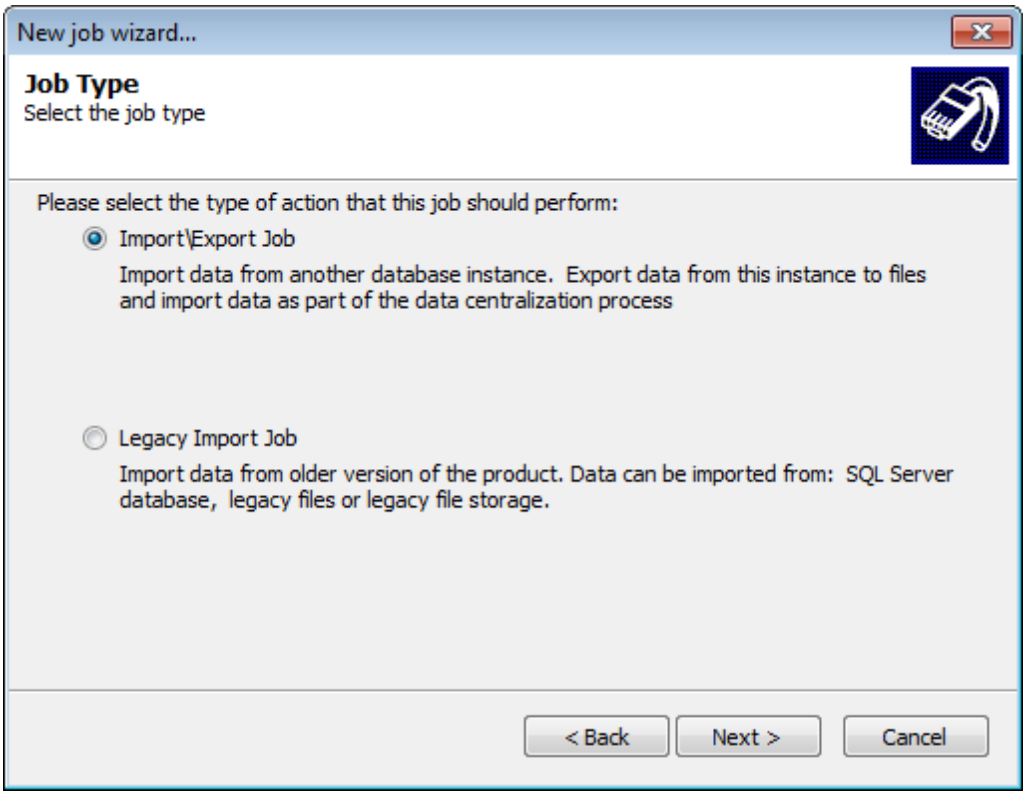
Table 89: Creating maintenance jobs - Schedule options

Options	Description
Schedule job	The job will be saved and executed according to the database operations schedule.
Run the job now	Job is executed immediately. Unscheduled jobs only run once and cannot be reused.

14.2.4 Copy data

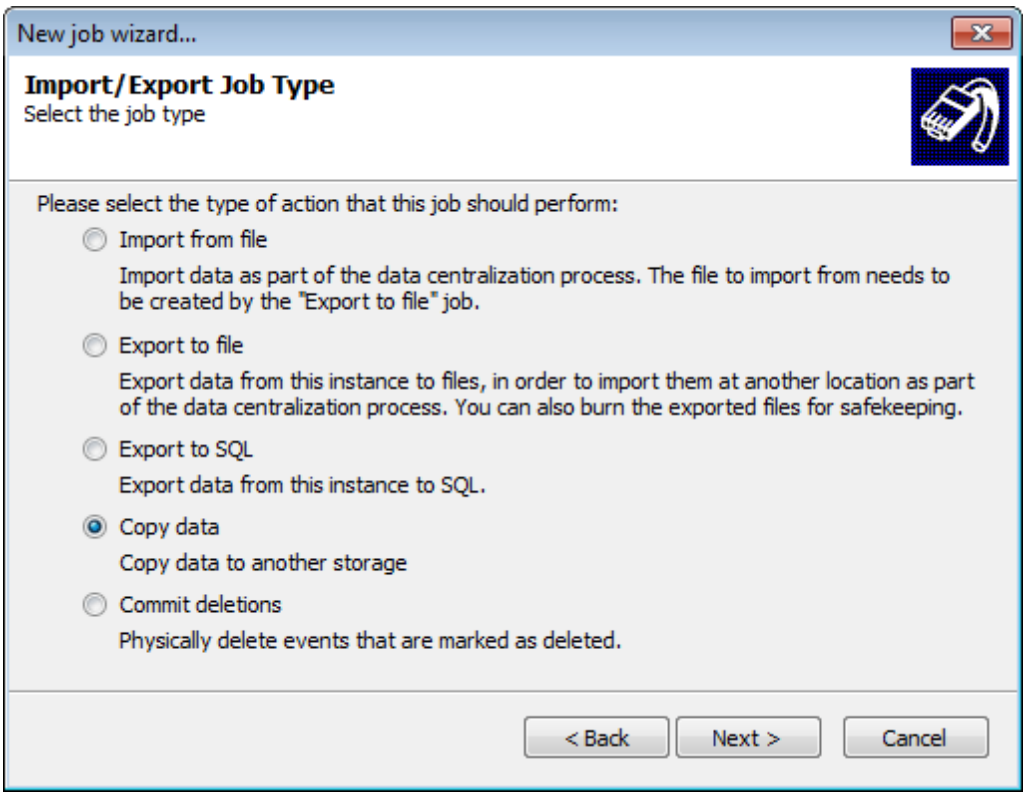
To create Copy data jobs:

1. Click **Configuration** tab and select **Options**.
2. From **Configurations**, right-click **Database Operations** node and select **Create new job…**
3. Click **Next** at the wizard welcome screen.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

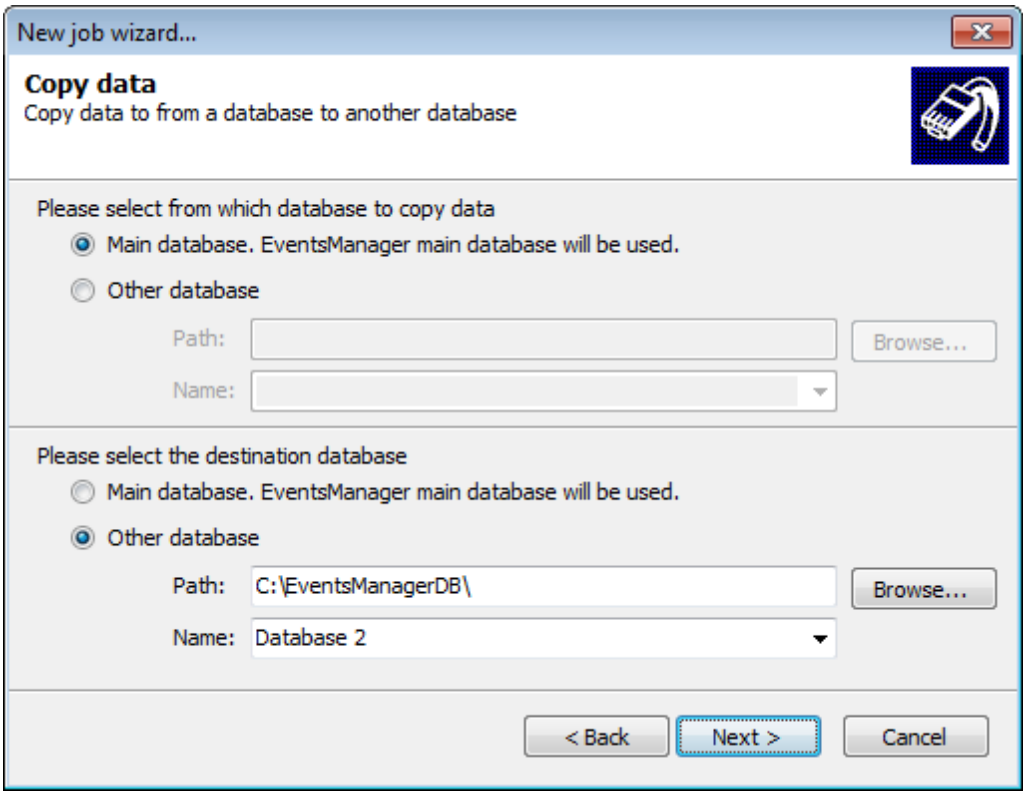
Screenshot 224: Creating Import\Export jobs

4. Select **Import/Export Job** and click **Next**.


New job wizard...
Import/Export Job Type
Select the job type
Please select the type of action that this job should perform:
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Export to SQL
Export data from this instance to SQL.
Copy data
Copy data to another storage
Commit deletions
Physically delete events that are marked as deleted.
< Back
Next >
Cancel

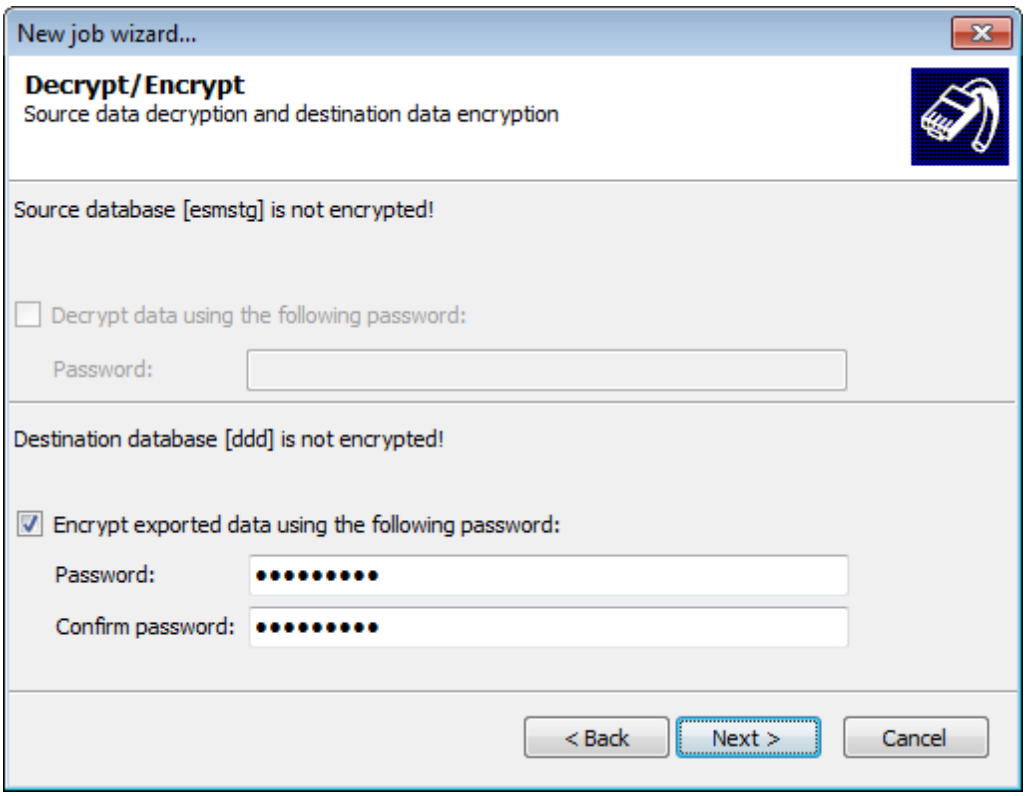
Screenshot 225: Select Copy data job

5. Select **Copy data** and click **Next**.



Screenshot 226: Specify source and destination databases

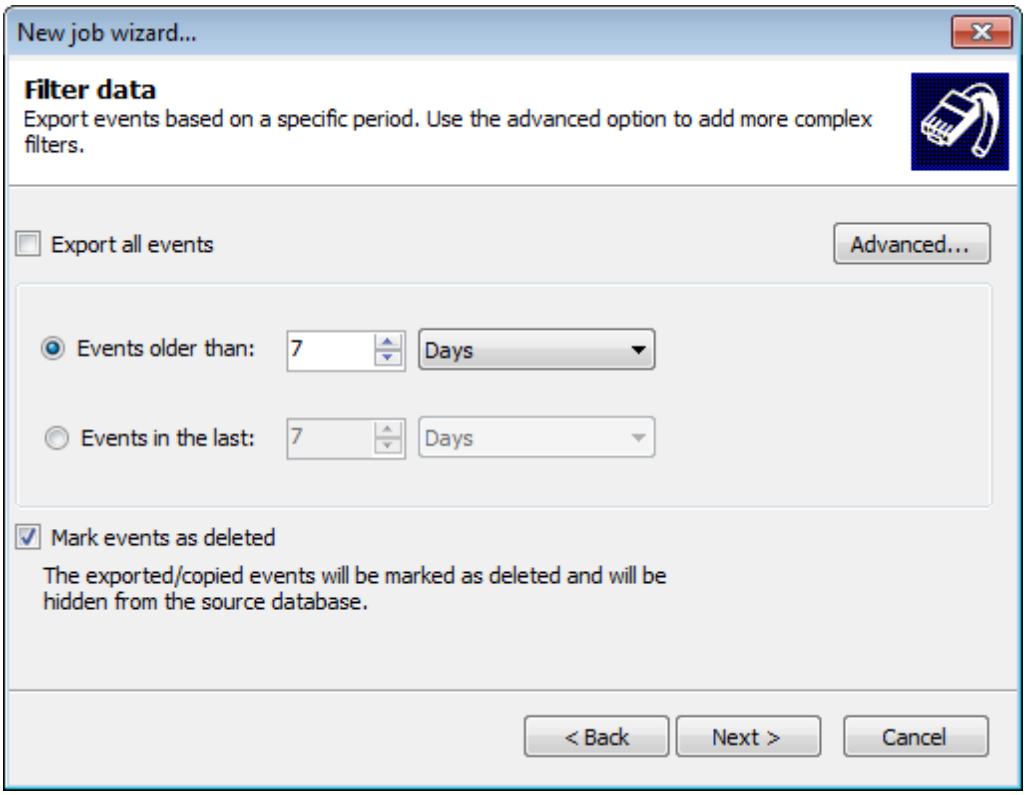
6. Select the source and destination databases. Click **Next**.



Screenshot 227: Decrypt source and encrypt destination databases

7. If the source database is encrypted, select **Decrypt data using the following password** and specify the password used to encrypt the database.

8. If you want to encrypt the source data, select **Encrypt exported data using the following password**. Specify the encryption password and click **Next**.


New job wizard...
Filter data
Export events based on a specific period. Use the advanced option to add more complex filters.
Export all events
Advanced...
Events older than:
7
Days
Events in the last:
7
Days
Mark events as deleted
The exported/copied events will be marked as deleted and will be hidden from the source database.
< Back
Next >
Cancel

Screenshot 228: Filtering export data

9. Configure the following filtering options and click **Next**:

Table 90: Filtering export data

Option	Description
Export all events	Export all events from the database.
Events older than	Only export events older than the specified number of days/weeks/months.
Events in the last	Only export events that occurred in the last specified number of days/weeks/months.
Mark events as deleted	Hide events from the source database after they are exported. To completely remove these events from the database, you must run a Commit Deletions job. For more information refer to Commit deletions.
Advanced...	Click Advanced... to launch the Advanced Filtering dialog. This enables you to configure granular filtering parameters to export specific events only. For more information refer to Building query restrictions.

10. Select when the job is executed and click **Finish**:

Table 91: Creating maintenance jobs - Schedule options

Options	Description
Schedule job	The job will be saved and executed according to the database operations schedule.
Run the job now	Job is executed immediately. Unscheduled jobs only run once and cannot be reused.

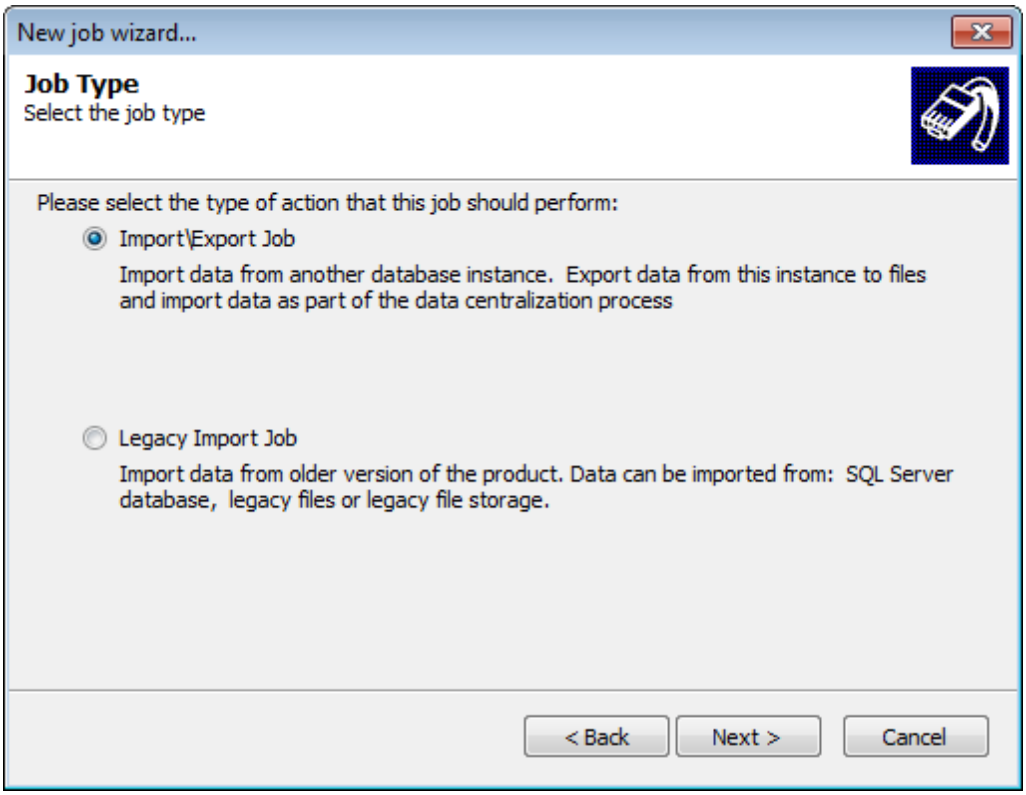
14.2.5 Commit deletions

To create Commit deletions jobs:

1. Click **Configuration** tab and select **Options**.

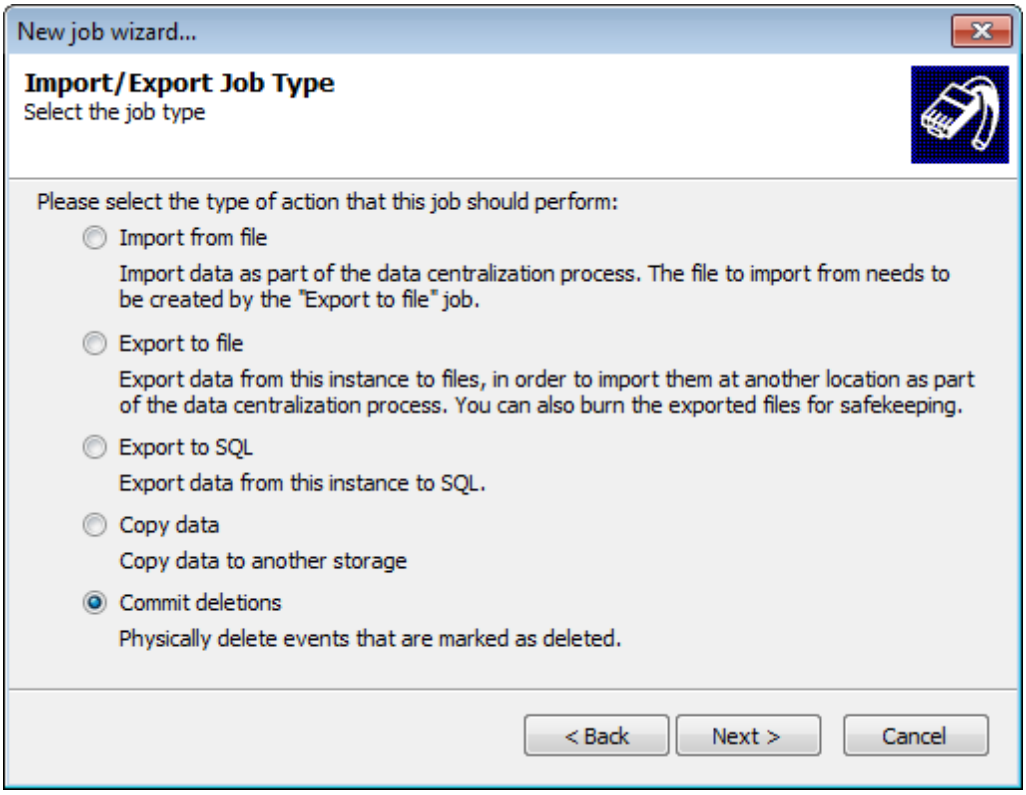
2. From **Configurations**, right-click **Database Operations** node and select **Create new job...**

3. Click **Next** at the wizard welcome screen.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

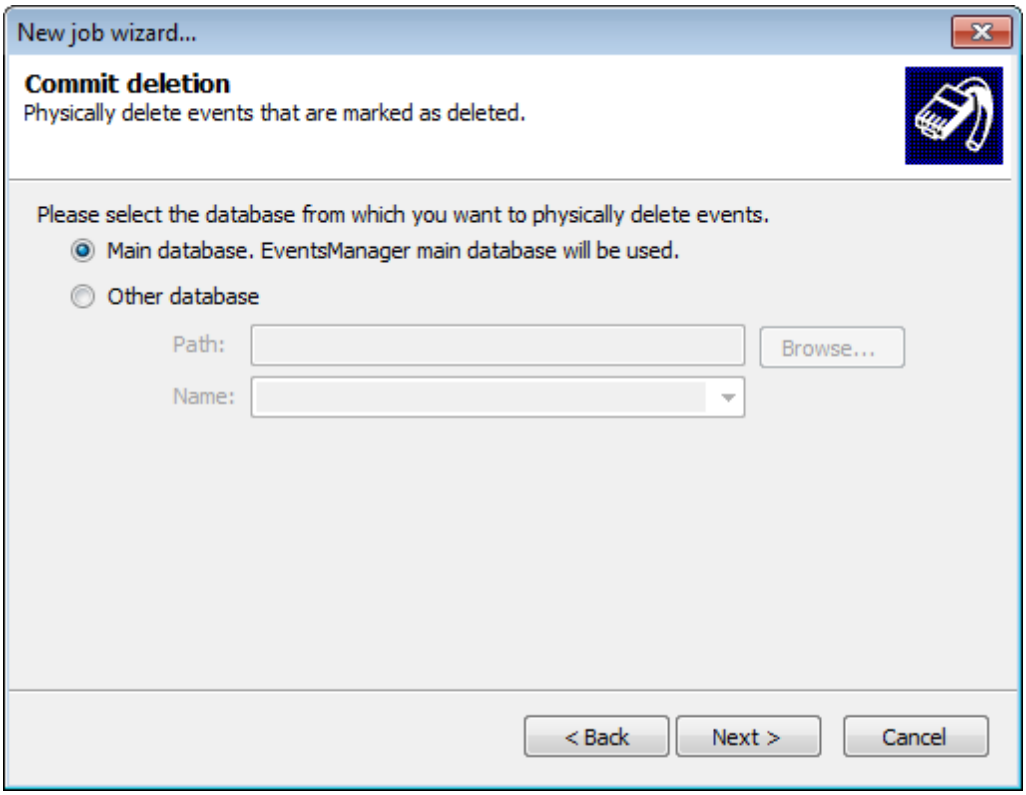
Screenshot 229: Creating Import\Export jobs

4. Select **Import/Export Job** and click **Next**.


New job wizard...
Import/Export Job Type
Select the job type
Please select the type of action that this job should perform:
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Export to SQL
Export data from this instance to SQL.
Copy data
Copy data to another storage
Commit deletions
Physically delete events that are marked as deleted.
< Back
Next >
Cancel

Screenshot 230: Create commit deletion jobs

5. Select **Commit deletions** and click **Next**.



Screenshot 231: Select database to delete records from

6. Select the database to delete records from. Click **Next**.

7. Select when the job is executed and click **Finish**:

Table 92: Creating maintenance jobs - Schedule options

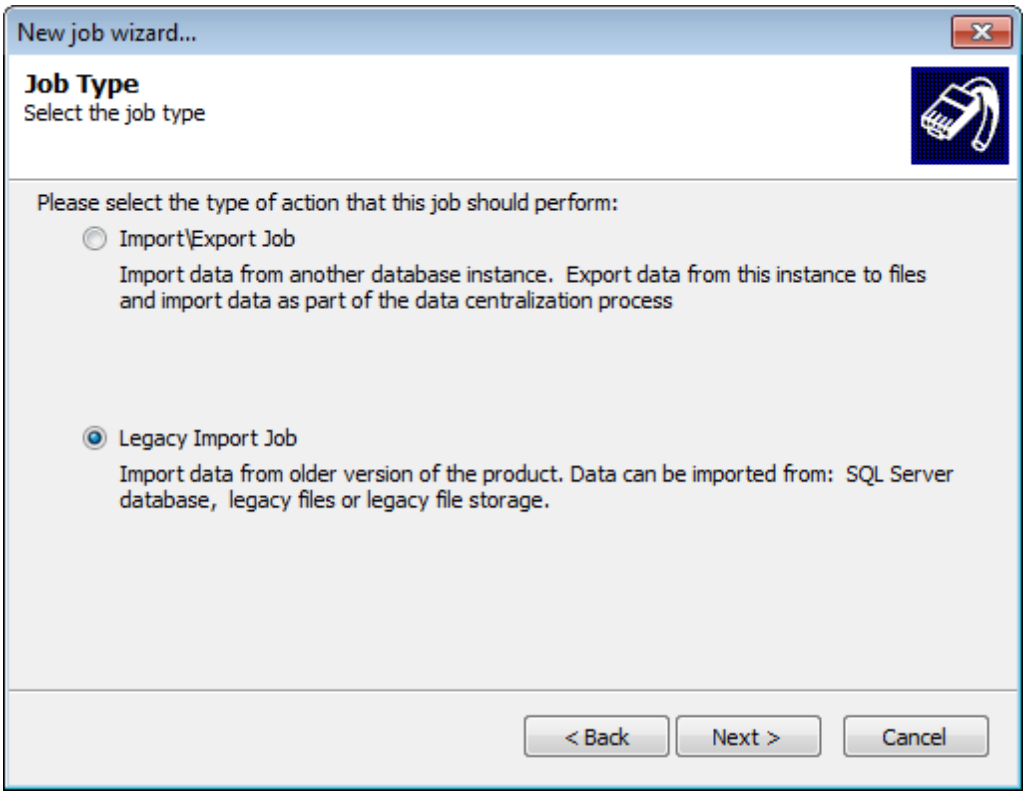
Options	Description
Schedule job	The job will be saved and executed according to the database operations schedule.
Run the job now	Job is executed immediately. Unscheduled jobs only run once and cannot be reused.

14.2.6 Import from SQL Server® Database

1. Click **Configuration** tab and select **Options**.

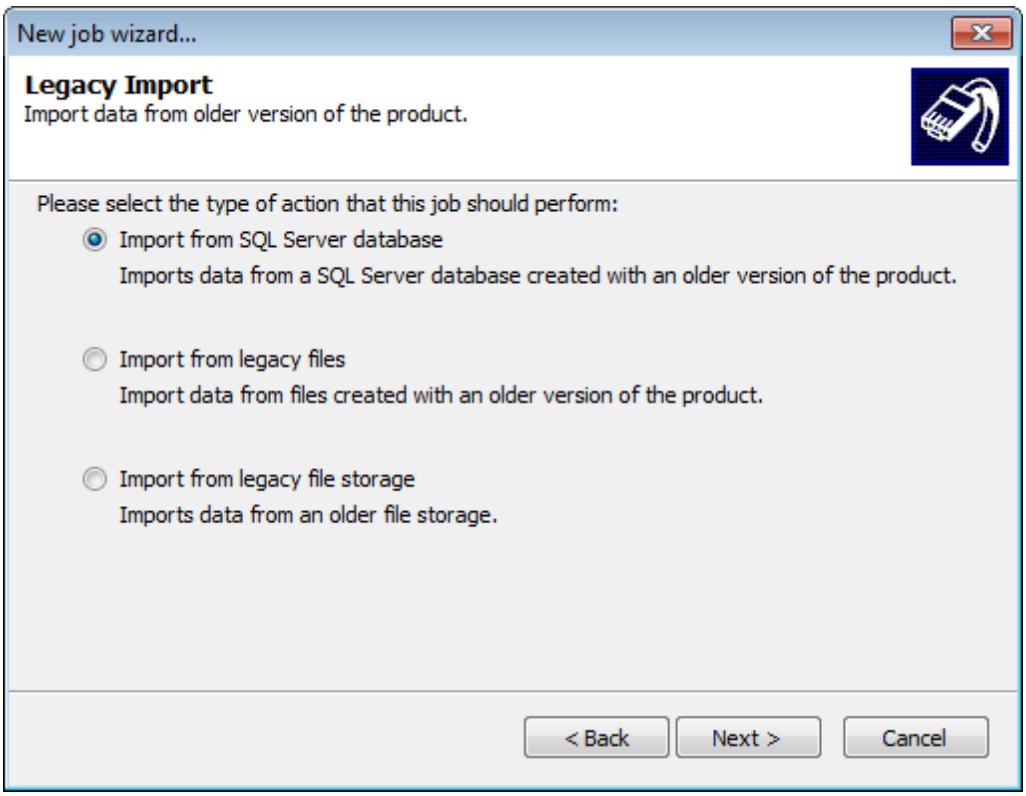
2. From **Configurations**, right-click **Database Operations** node and select **Create new job…**

3. Click **Next** at the wizard welcome screen.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

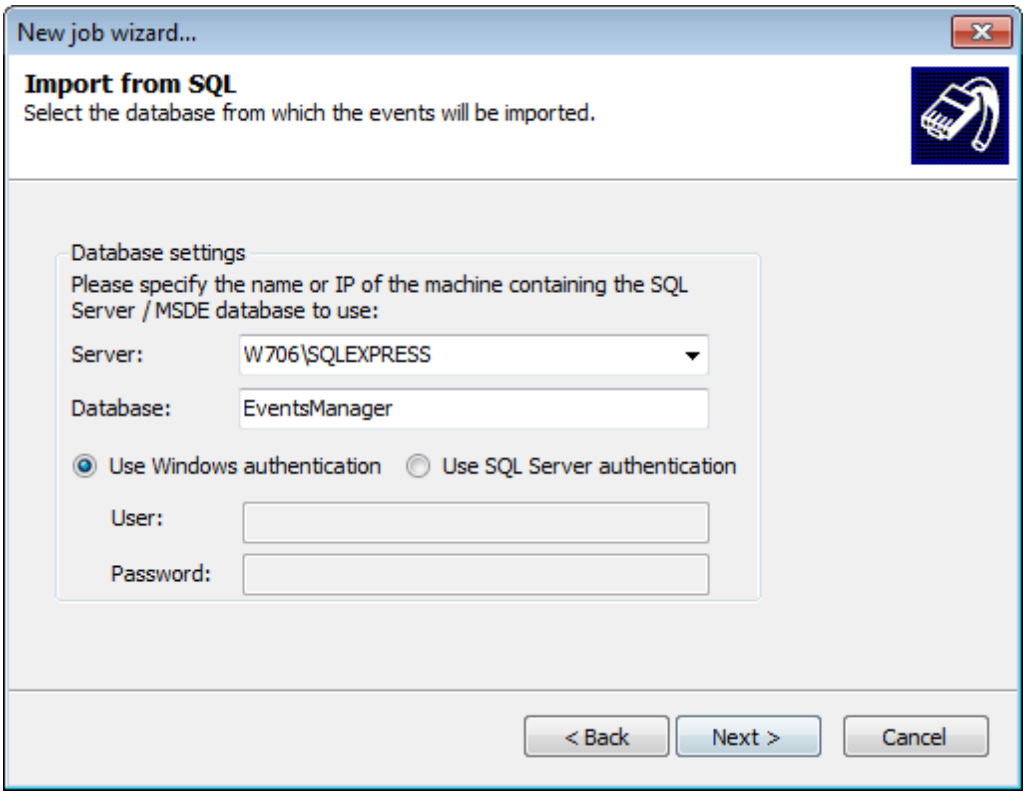
Screenshot 232: Creating Import\Export jobs

4. Select **Legacy Import Job** and click **Next**.


New job wizard...
Legacy Import
Import data from older version of the product.
Please select the type of action that this job should perform:
Import from SQL Server database
Imports data from a SQL Server database created with an older version of the product.
Import from legacy files
Import data from files created with an older version of the product.
Import from legacy file storage
Imports data from an older file storage.
< Back
Next >
Cancel

Screenshot 233: Select Import from SQL Server Database

5. Select **Import from SQL Server® database** and click **Next**.

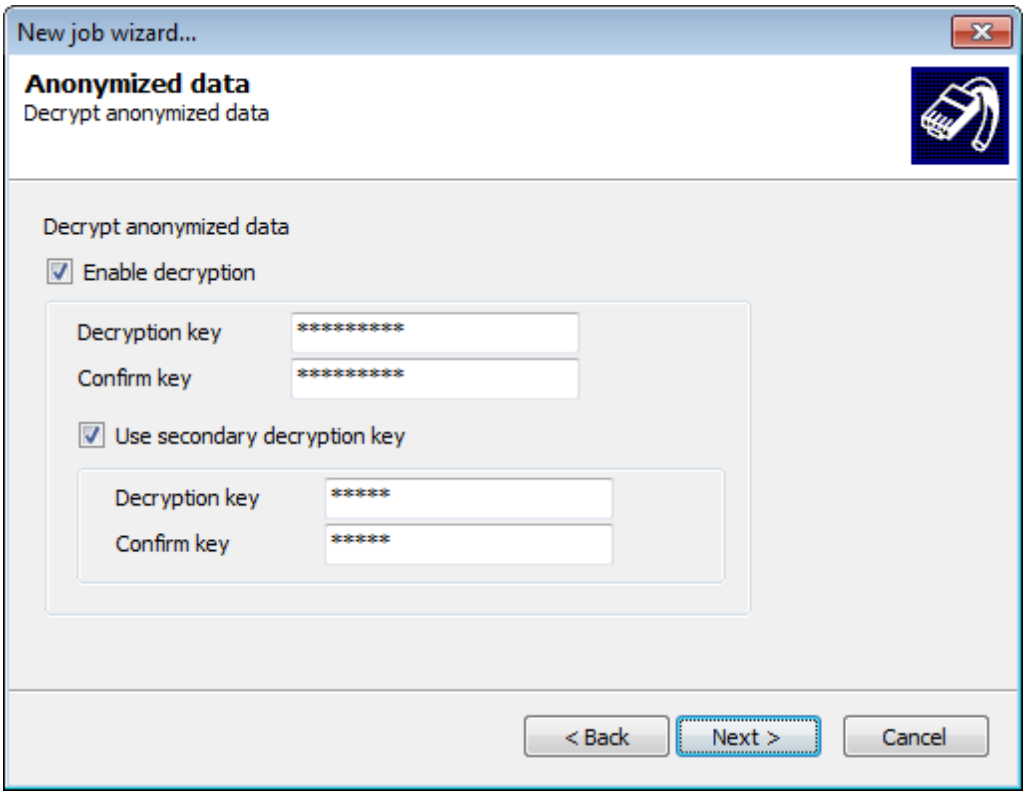


Screenshot 234: Specify SQL Server address and login details

6. Configure the following server options and click **Next**:

Table 93: Export to SQL - Server options

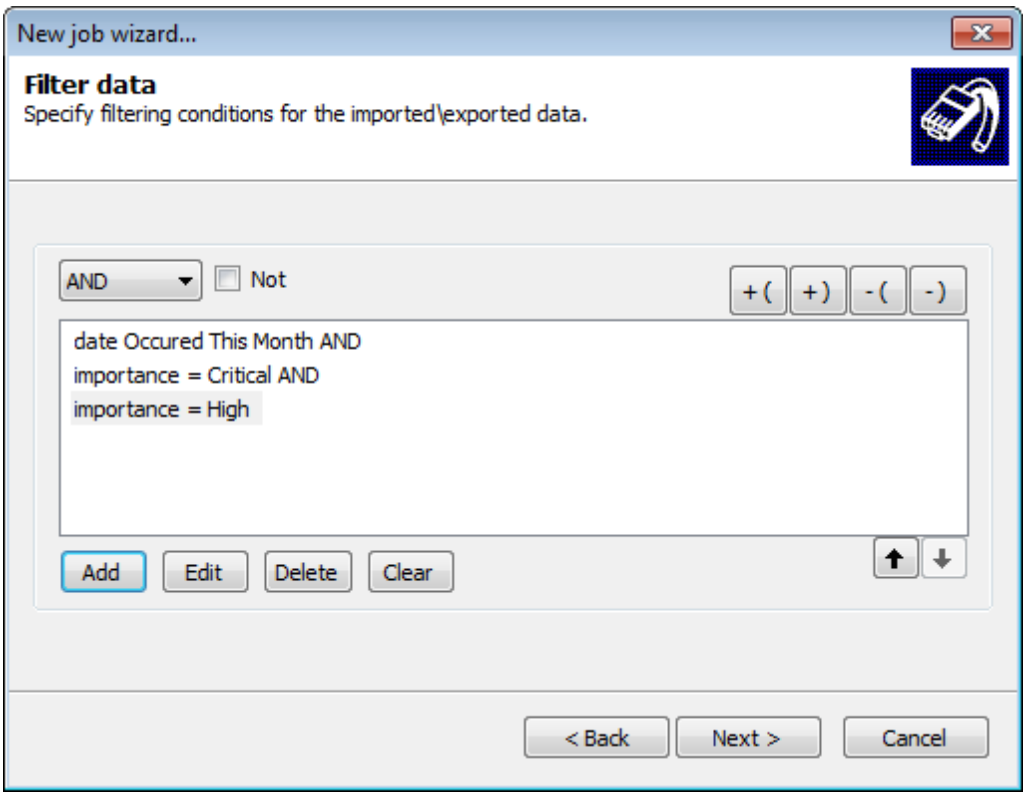
Option	Description
Server	Key in the name of the machine that is running SQL Server.
Database	Key in the name of the source database.
Use Windows authentication	Use the same logon credentials used to log on to Windows®. The SQL Server® must support this type of authentication mode to be able to connect and copy information from the server.
Use SQL Server authentication	Use the logon credentials configured in your SQL Server®. Key in the username in the **User** field and the password in the **Password** field.



Screenshot 235: Decrypt anonymized databases

7. (Optional) If the SQL Server® database is anonymized, select **Enable decryption** and specify the password used to anonymize the database.

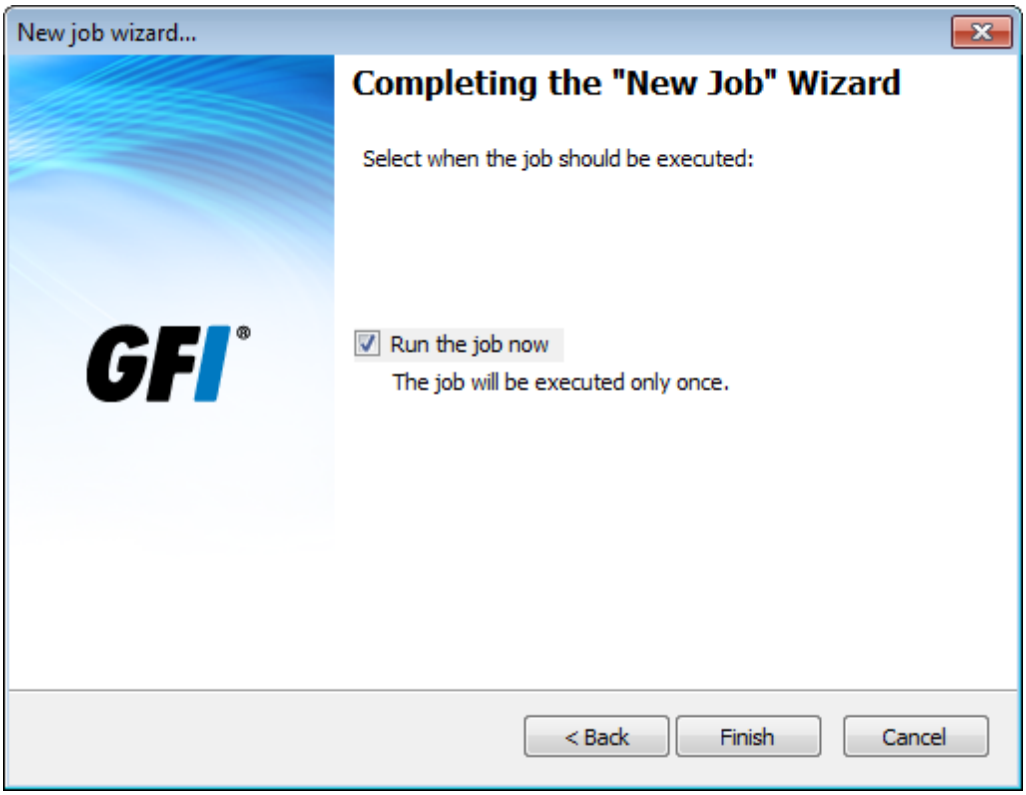
8. (Optional) If the SQL Server database was anonymized using two password, select **Use secondary decryption key** and specify the second security password used to anonymize the database. Click **Next**.



Screenshot 236: Add filtering conditions to filter unwanted data

9. Add advanced filtering parameters to import specific data only. Leave blank to import all the event logs.

> **Note**
>
> For more information refer to Building Query Restrictions.



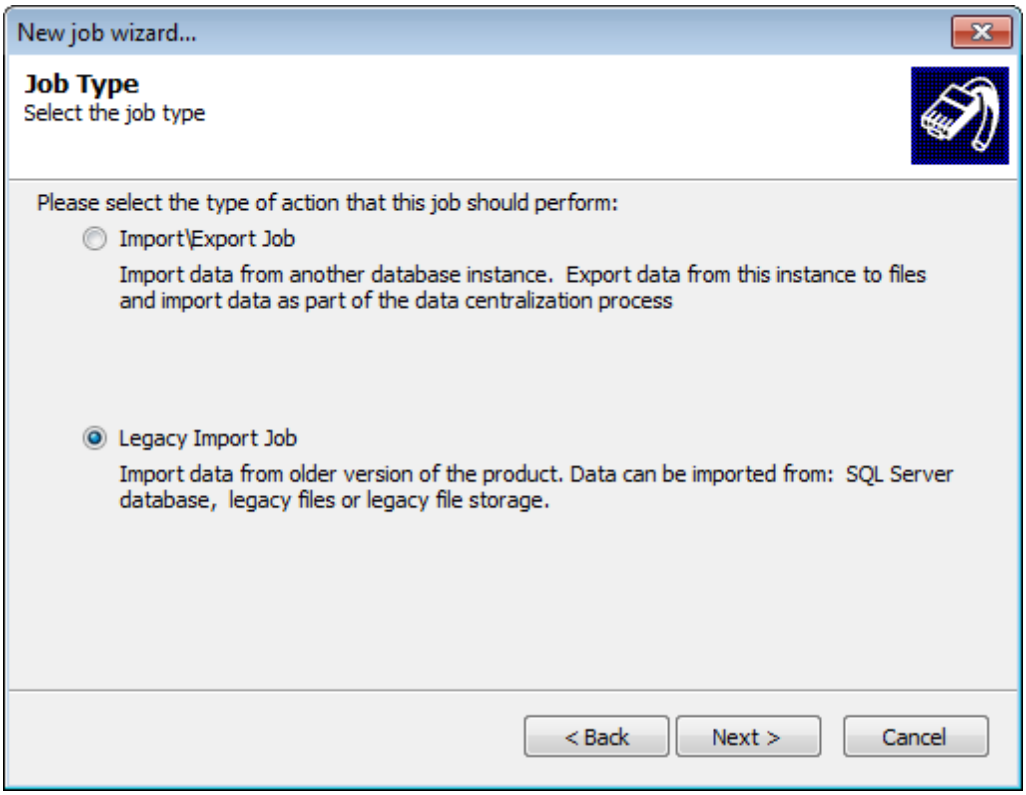
Screenshot 237: Specify when the maintenance job is executed

Select **Run the job now** and click **Finish**.

14.2.7 Import from legacy files

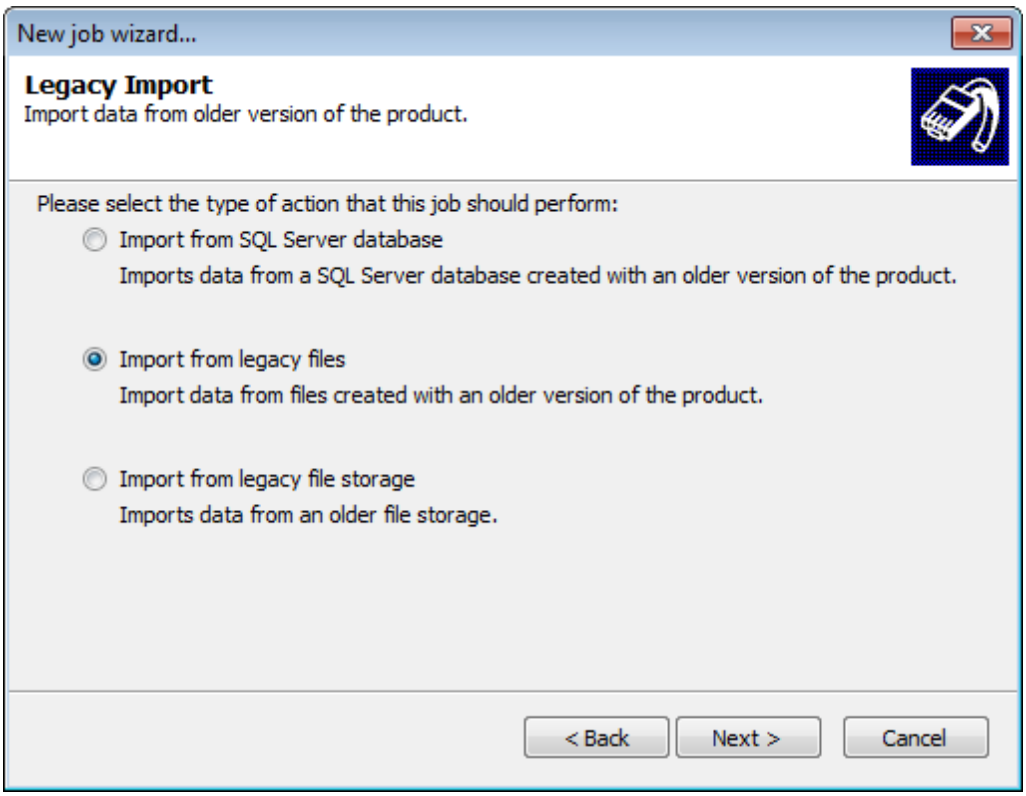
To create Import from legacy files jobs:

1. Click **Configuration** tab and select **Options**.
2. From **Configurations**, right-click **Database Operations** node and select **Create new job…**
3. Click **Next** at the wizard welcome screen.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

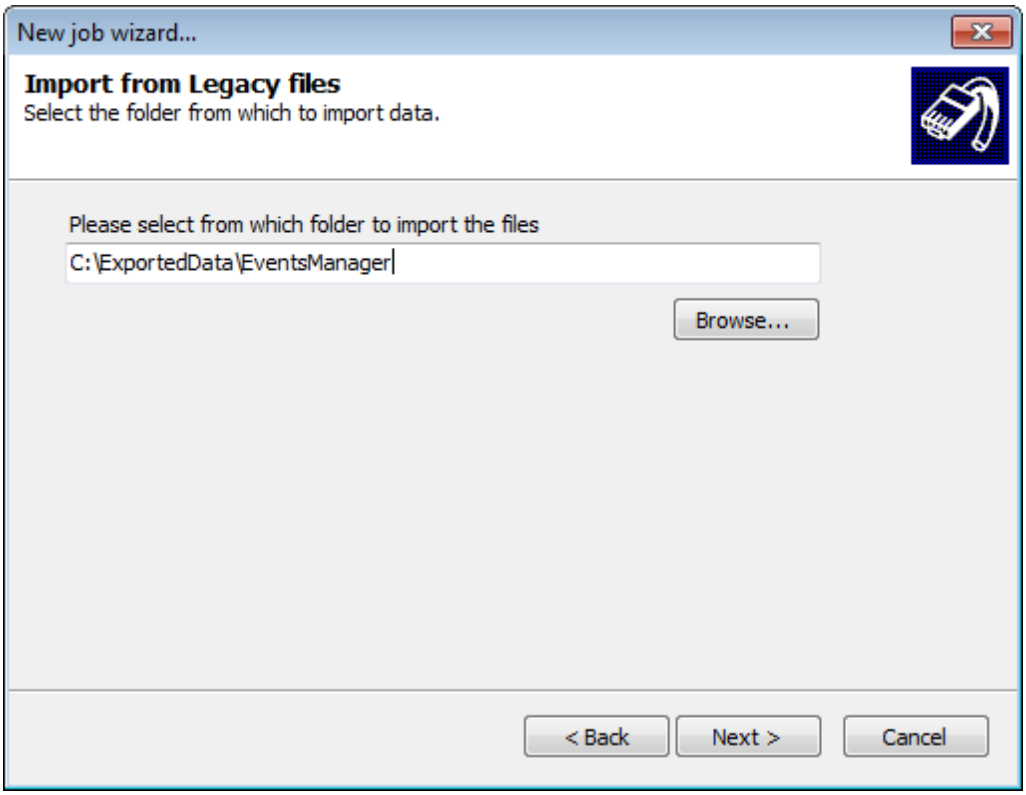
Screenshot 238: Creating Import\Export jobs

4. Select **Legacy Import Job** and click **Next**.


New job wizard...
Legacy Import
Import data from older version of the product.
Please select the type of action that this job should perform:
Import from SQL Server database
Imports data from a SQL Server database created with an older version of the product.
Import from legacy files
Import data from files created with an older version of the product.
Import from legacy file storage
Imports data from an older file storage.
< Back
Next >
Cancel

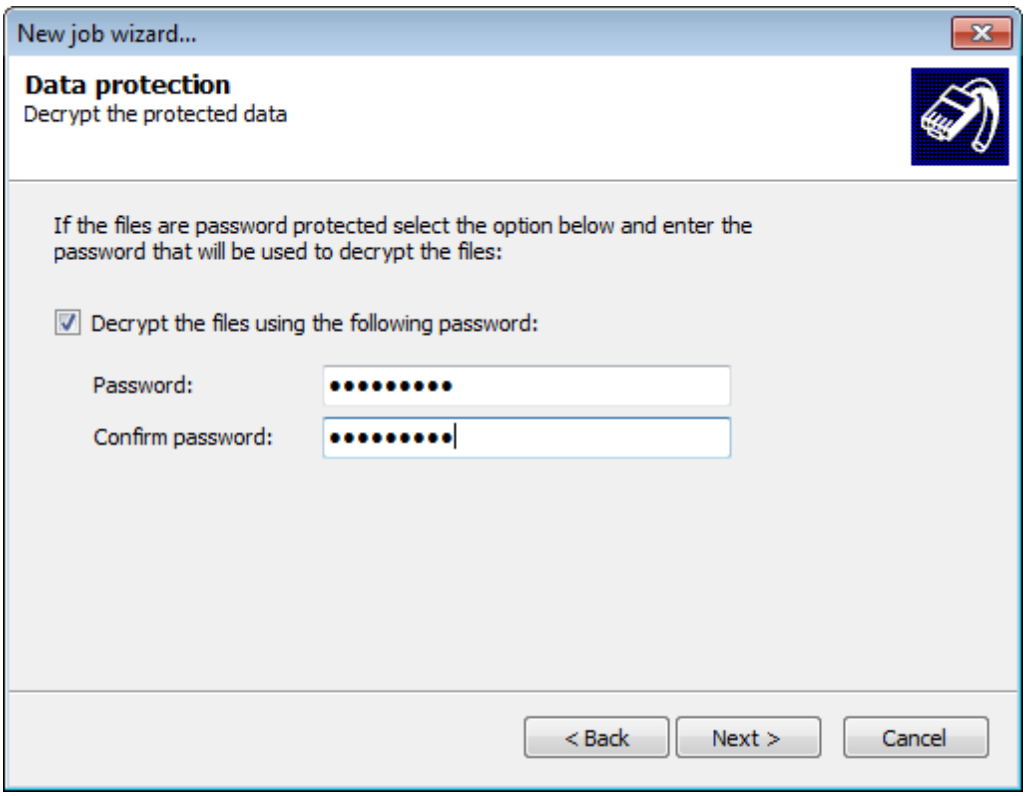
Screenshot 239: Import from legacy files

5. Select **Import from legacy files** and click **Next**.



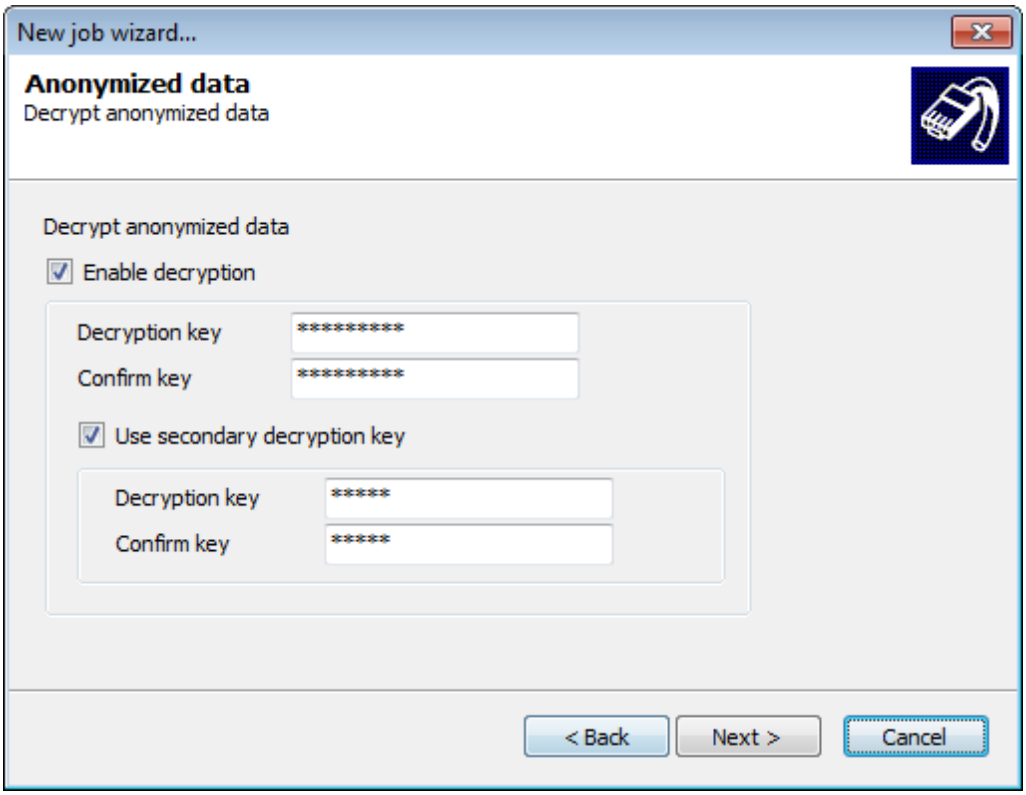
Screenshot 240: Specify import file location

6. Specify the path to the configuration file that contains data you want to import. Optionally, click **Browse** to look for the location. Click **Next**.


New job wizard...
Data protection
Decrypt the protected data
If the files are password protected select the option below and enter the password that will be used to decrypt the files:
Decrypt the files using the following password:
Password:
Confirm password:
< Back
Next >
Cancel

Screenshot 241: Decrypt the information in the import file

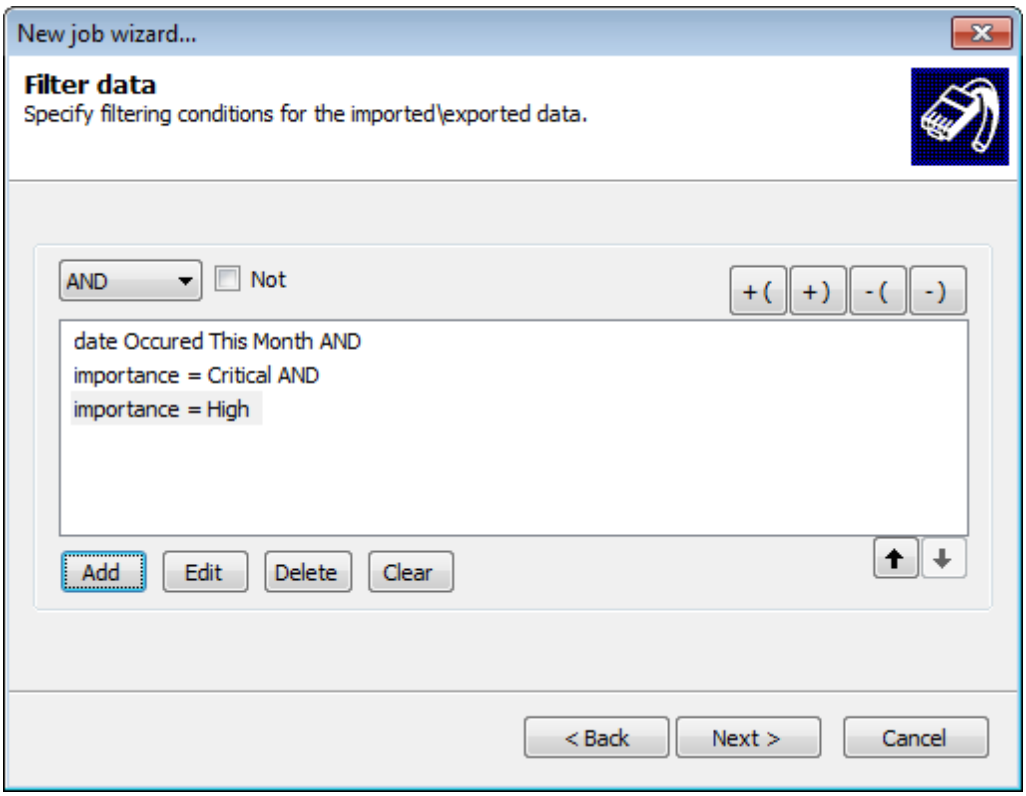
7. (Optional) If the file was encrypted, select **Decrypt the files using the following password** and specify the password used to encrypt the file. Click **Next**.



Screenshot 242: Remove anonymization

8. (Optional) If the file is anonymized, select **Enable decryption** and specify the password used to anonymize the data.

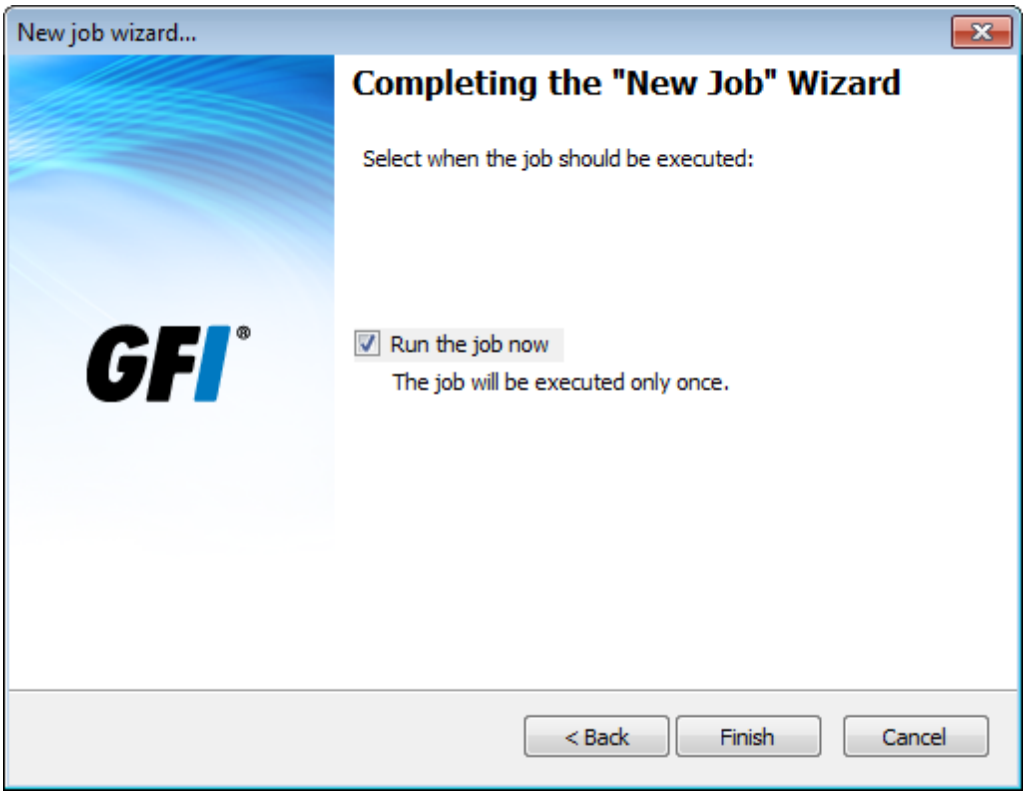
9. (Optional) If the file was anonymized using two passwords, select **Use secondary decryption key** and specify the second key used to anonymize the data within the file. Click **Next**.



Screenshot 243: Filter unwanted events through filtering conditions

10. Add advanced filtering parameters to import specific data only. Leave blank to import all the event logs.

> **Note**
>
> For more information refer to Building Query Restrictions.



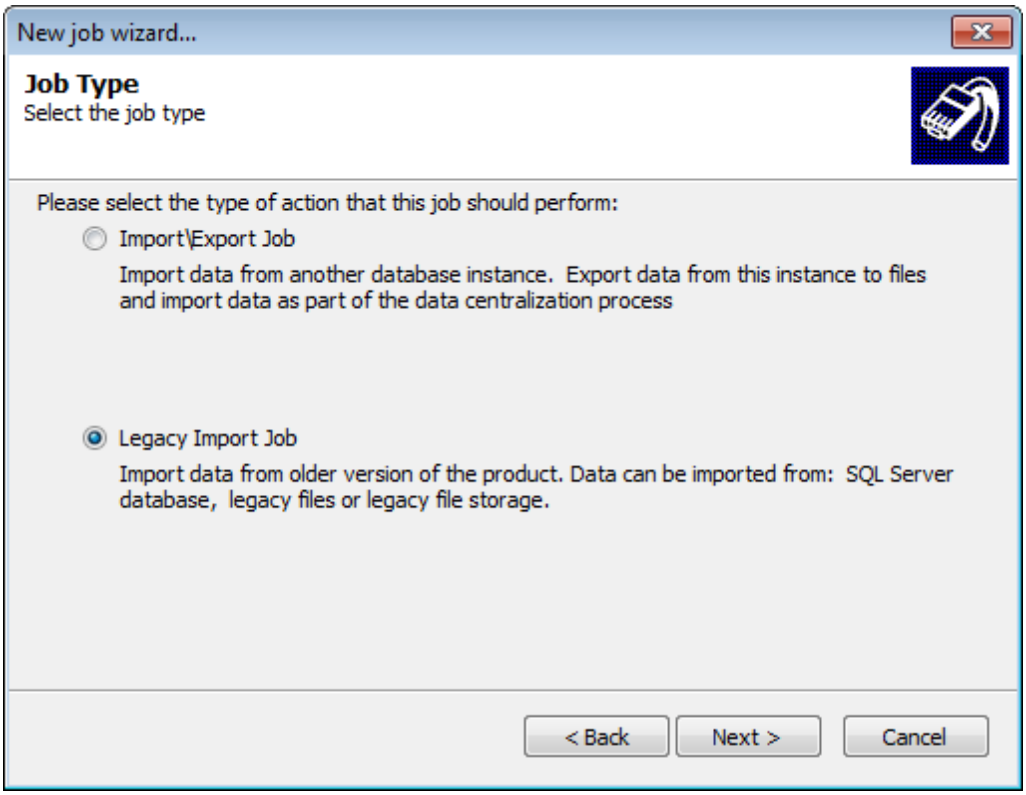
Screenshot 244: Specify when the maintenance job is executed

Select **Run the job now** and click **Finish**.

14.2.8 Import from legacy file storage

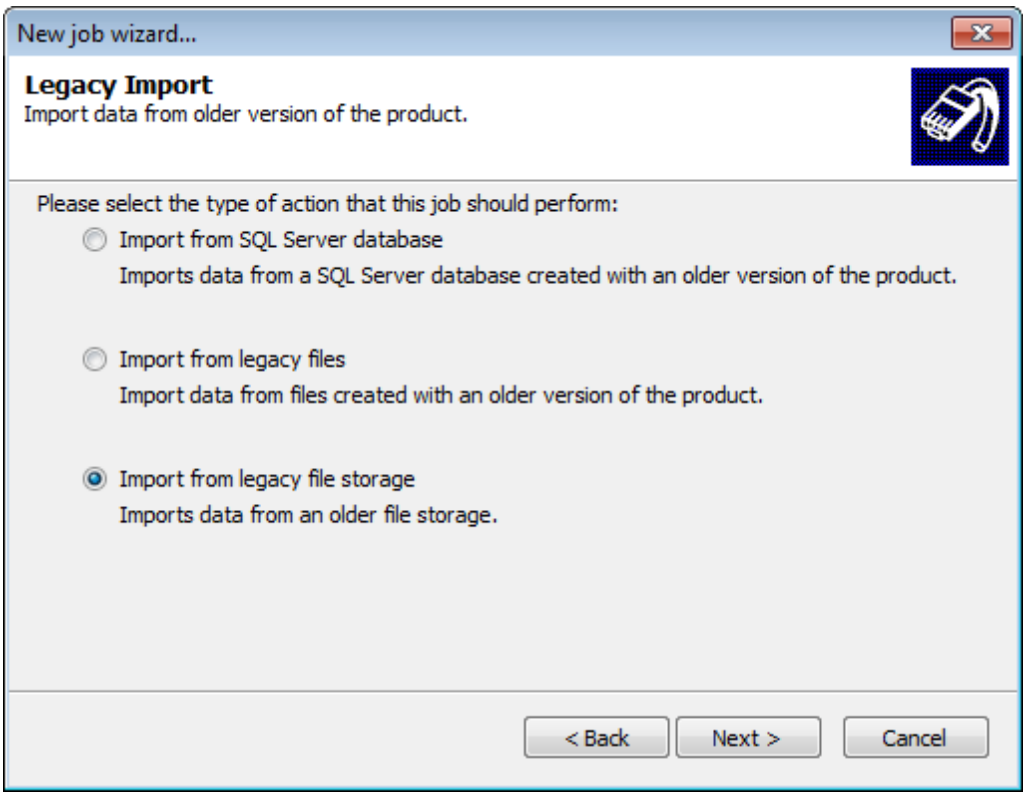
To create Import from legacy files jobs:

1. Click **Configuration** tab and select **Options**.
2. From **Configurations**, right-click **Database Operations** node and select **Create new job…**
3. Click **Next** at the wizard welcome screen.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

Screenshot 245: Creating Import\Export jobs

4. Select **Legacy Import Job** and click **Next**.


New job wizard...
Legacy Import
Import data from older version of the product.
Please select the type of action that this job should perform:
Import from SQL Server database
Imports data from a SQL Server database created with an older version of the product.
Import from legacy files
Import data from files created with an older version of the product.
Import from legacy file storage
Imports data from an older file storage.
< Back
Next >
Cancel

Screenshot 246: Import legacy file storage data

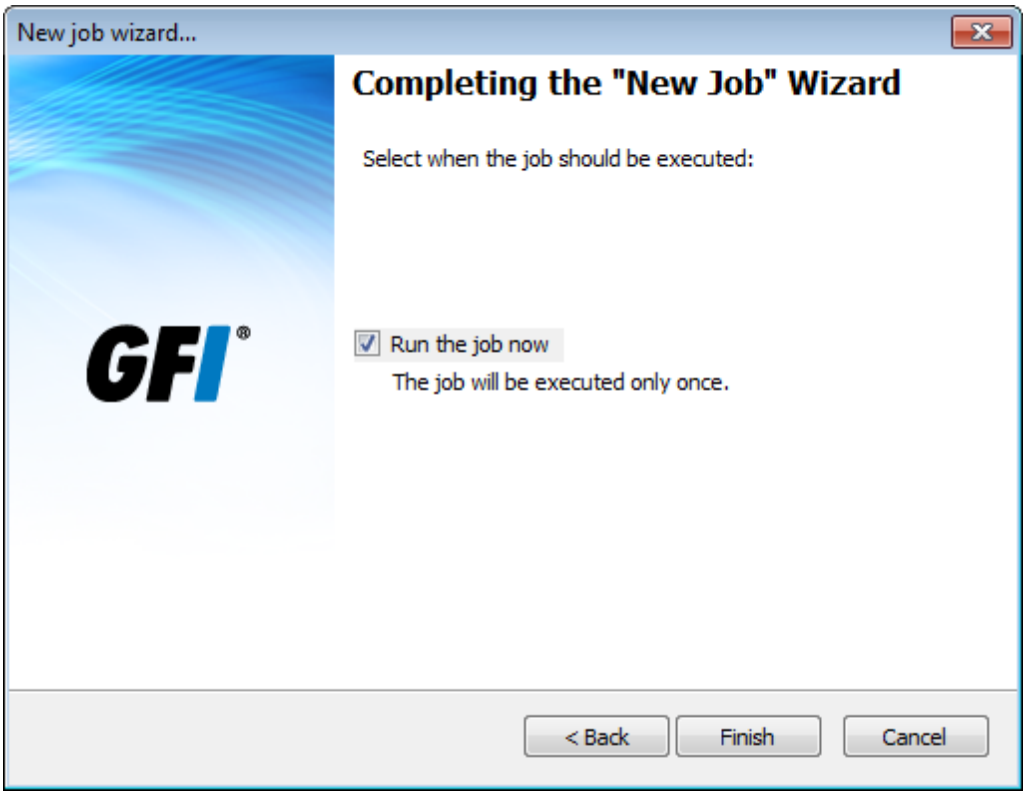
5. Select **Import from legacy file storage** and click **Next**.

6. Specify the path to where the import file is located. Alternatively, click **Browse** and look for the location.

7. (Optional) If the data is anonymized, select **Enable decryption** and specify the password used to encrypt the data.

8. (Optional) If the data is encrypted by two passwords, select **Use secondary decryption** key and key in the secondary password. Click **Next**.

9. (Optional) Specify filtering conditions to filter out unwanted data. Leave it blank to export all the data in the database. For more information, refer to Defining Restrictions. Click **Next**.



Screenshot 247: Specify when the maintenance job is executed

Select **Run the job now** and click **Finish**.

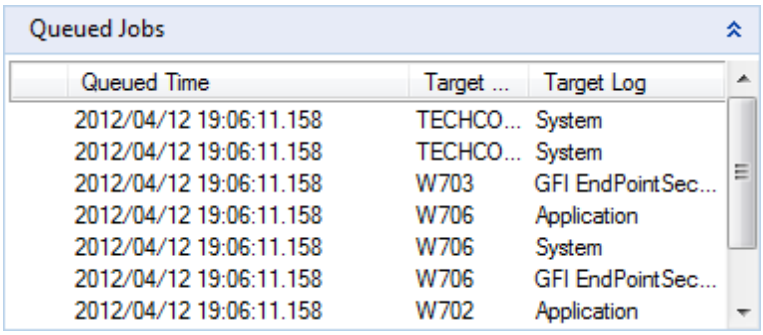
14.3 Editing maintenance jobs

This section contains information about:

- Viewing scheduled maintenance jobs
- Editing maintenance job properties
- Changing maintenance jobs priority
- Deleting a maintenance job

14.3.1 Viewing scheduled maintenance jobs

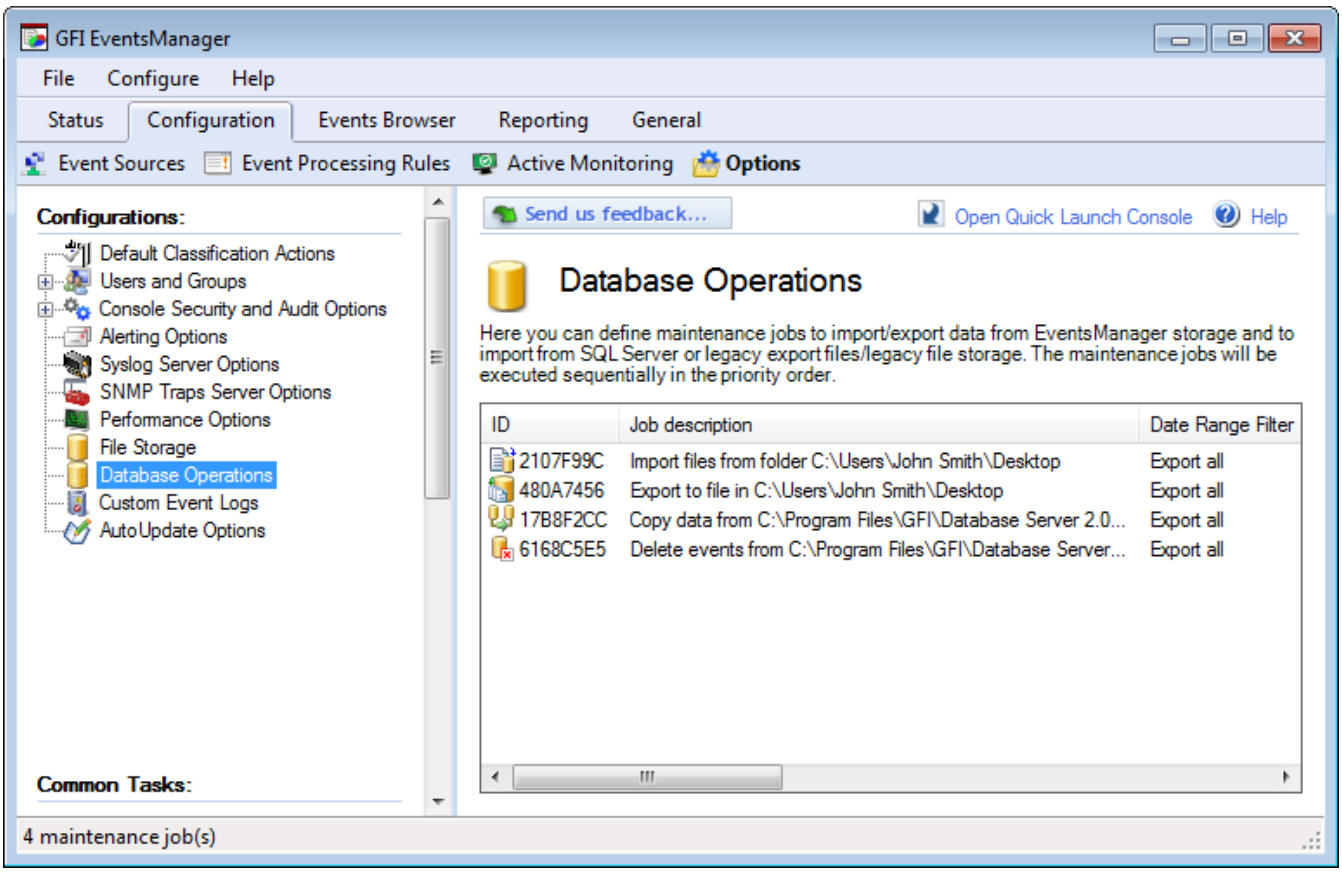
To view the progress of scheduled maintenance jobs:



Screenshot 248: Maintenance job activity

Click **Status** tab > **Job Activity**. The status of all maintenance jobs will be displayed in the **Queued Jobs** section.

To view created maintenance jobs:



Screenshot 249: Viewing scheduled maintenance jobs

1. Click **Configuration** tab and select **Options**.

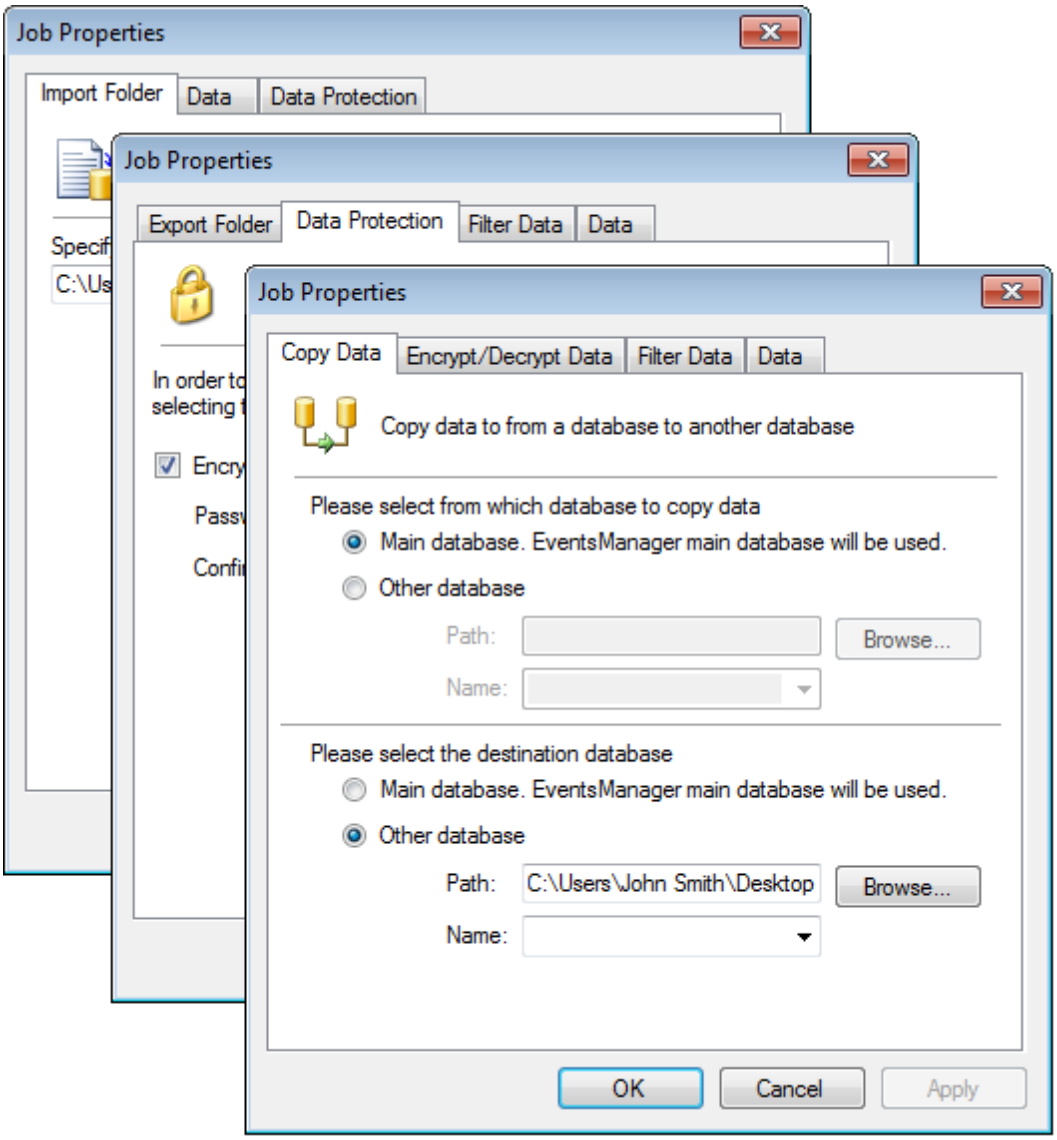
2. From **Configurations**, select the **Database Operations** node. Scheduled maintenance jobs are displayed in the right pane.

14.3.2 Editing maintenance job properties

To edit maintenance jobs properties:

1. From **Configuration** tab > **Options** > **Configurations**, click **Database Operations**.

2. From the right pane, right-click on a maintenance job and select **Properties**.



Screenshot 250: Maintenance job properties dialog

3. From the Job Properties dialog, you can modify the settings you configured while creating the job; such as:

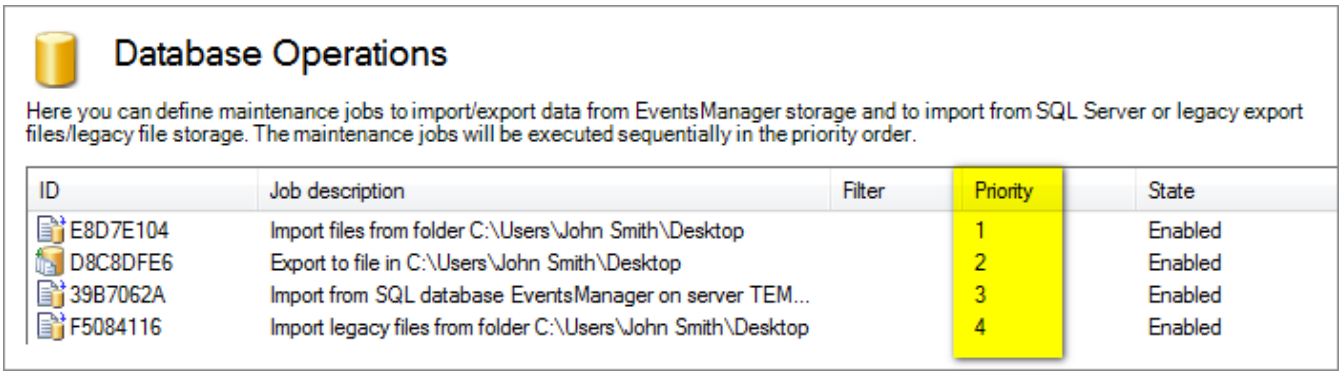
- Encryption/decryption passwords
- Database names and addresses
- Source/destination paths
- General job details.

4. Click **Apply** and **OK**.

Note

For more information refer to Creating maintenance jobs.

14.3.3 Changing maintenance jobs priority



Screenshot 251: Maintenance job priorities

By default maintenance jobs are executed according to the sequence with which the jobs are created (First-in-First-out). Thus the priority of maintenance jobs is determined by the sequence in which jobs are executed.

To increase or decrease the priority of a maintenance job:

1. Click **Configuration** tab and select **Options**.

2. From **Configurations**, select **Database Operations** node.

3. From the right pane, right-click the maintenance job and select **Increase Priority** or **Decrease Priority** accordingly.

14.3.4 Deleting a maintenance job

To delete maintenance jobs:

1. Click **Configuration** tab and select **Options**.

2. From **Configurations**, select **Database Operations** node.

3. From the right pane, right-click on the maintenance job to delete and select **Delete**.

> **Note**
>
> Before deleting maintenance jobs ensure that all data is backed up.

15 Configuring the Management Console

This chapter provides you with information about configuring general settings of GFI EventsManager, such as product licensing, performance options and product updates.

Topics in this chapter:

15.1 Performance options 285

15.2 Product updates 286

15.3 Product licensing 293

15.4 Product version information 294

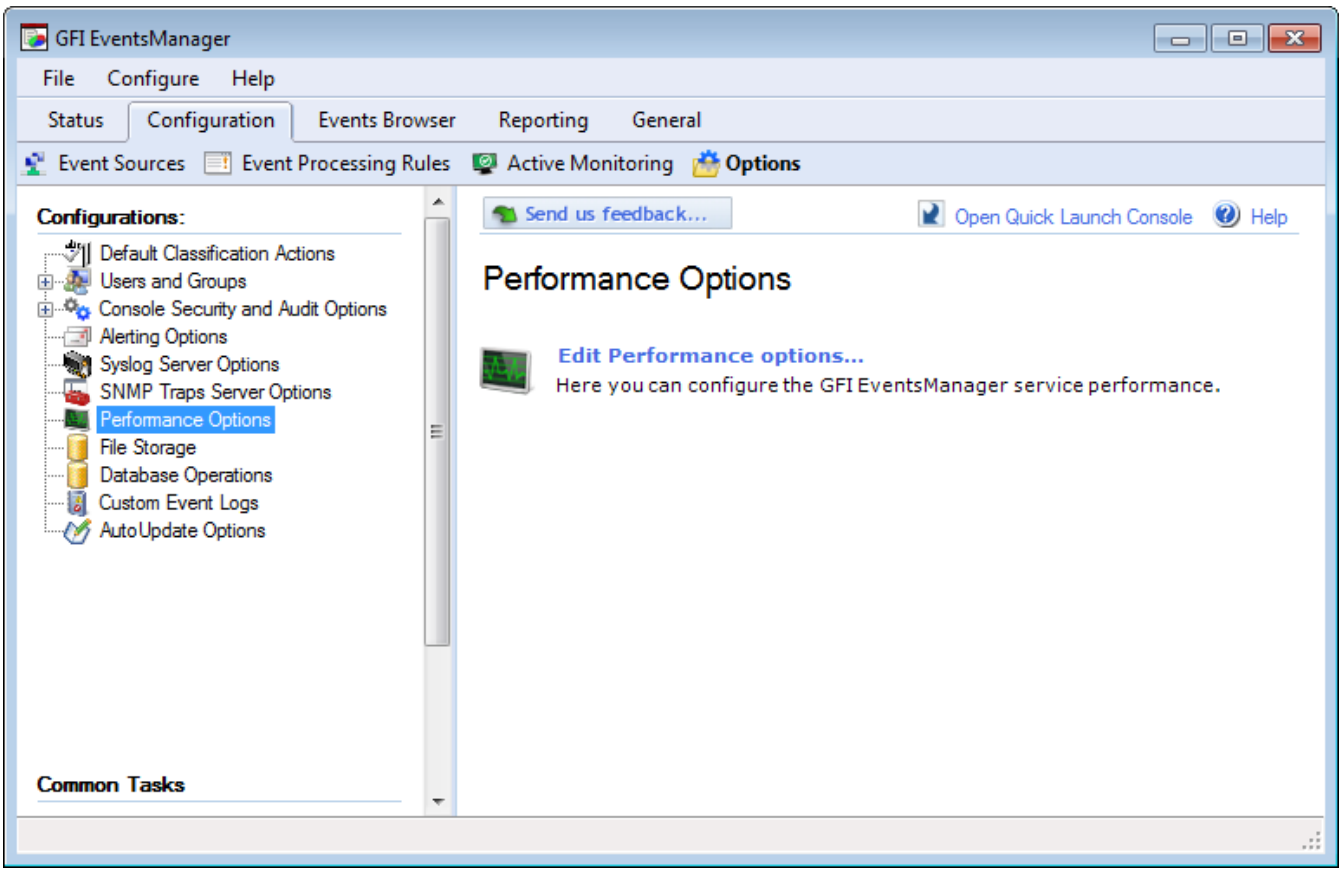
15.5 Importing and Exporting settings 295

15.6 Building query restrictions 302

15.1 Performance options

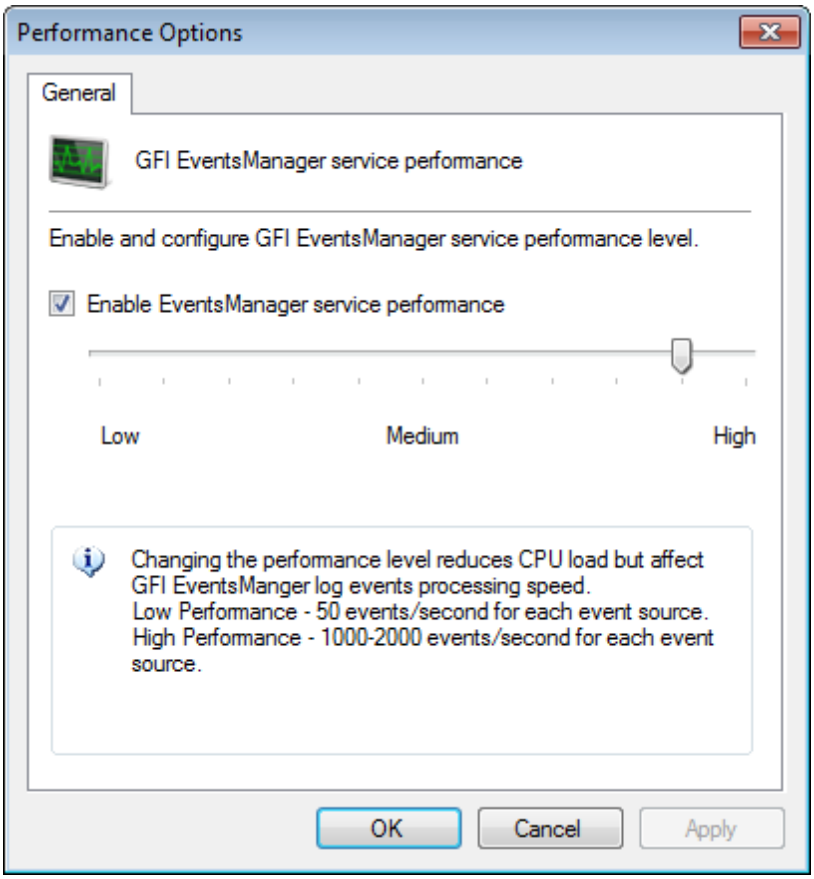
GFI EventsManager provides you with options which enable you to set the performance level of the GFI EventsManager service.

To configure the performance level:



Screenshot 252: GFI EventsManager Performance Options

1. From **Configuration** tab > **Options** > **Configurations**, right-click **Performance Options** and select **Edit Performance Options**.


Performance Options
General
GFI EventsManager service performance
Enable and configure GFI EventsManager service performance level.
Enable EventsManager service performance
Low
Medium
High
Changing the performance level reduces CPU load but affect GFI EventsManger log events processing speed.
Low Performance - 50 events/second for each event source.
High Performance - 1000-2000 events/second for each event source.
OK
Cancel
Apply

Screenshot 253: Performance Options dialog

2. Select/Unselect **Enable EventsManager service performance** to enable/disable service performance options.

3. Move the slider left (low) to right (high) until you reach the required performance level.

4. Click **Apply** and **OK**.

> **Note**
>
> Setting the performance level on **low** is estimated to process **50 events per second per event source**, while setting the bar on **high** processes **1,000 - 2,000 events per second per event source**.

15.2 Product updates

Periodically, GFI releases product updates to improve or add functionality to GFI EventsManager. Product updates are important to download and install because they fix issues with underlying technologies as well as increase compatibility with different technologies and devices.

When the GFI EventsManager host is connected to the Internet, products updates can be downloaded directly from the Management Console. Where Internet access is limited or there is none at all, product updates can be downloaded from an alternate location and then placed in the updates repository manually. Refer to the following sections for information about:

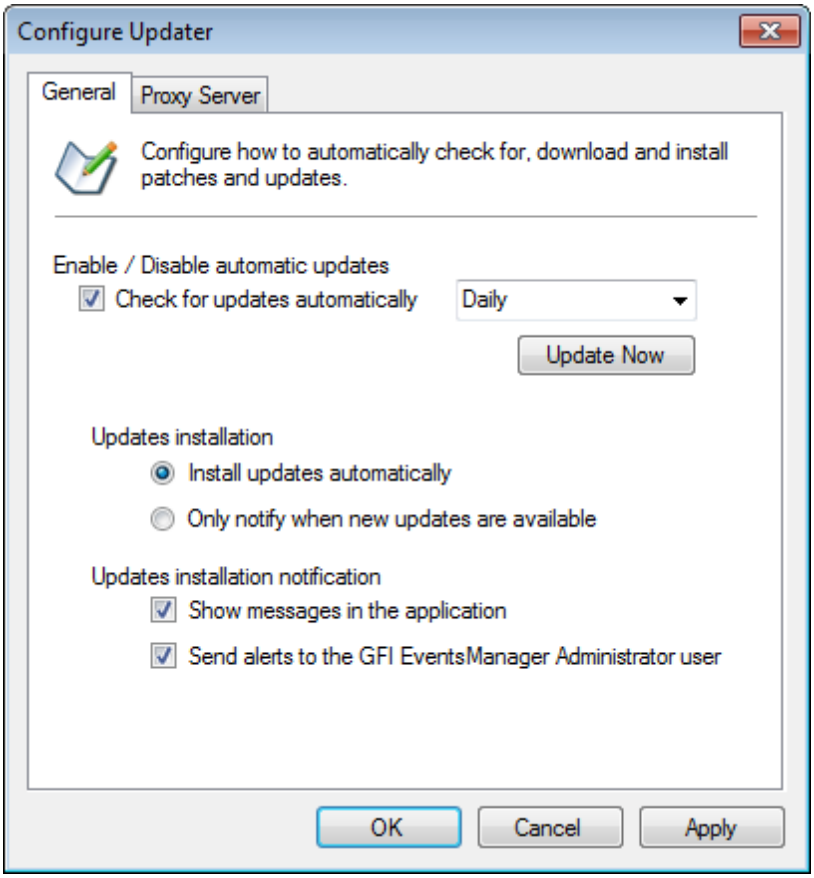
- Downloading updates directly
- Downloading updates from an alternate location (offline)

15.2.1 Downloading updates directly

GFI EventsManager enables users to configure how to automatically check for, download and install product updates.

To configure Auto Update options:

1. From **Configuration** tab > **Options** > **Configurations**, right-click **Auto Update Options** and select **Edit updater options...**



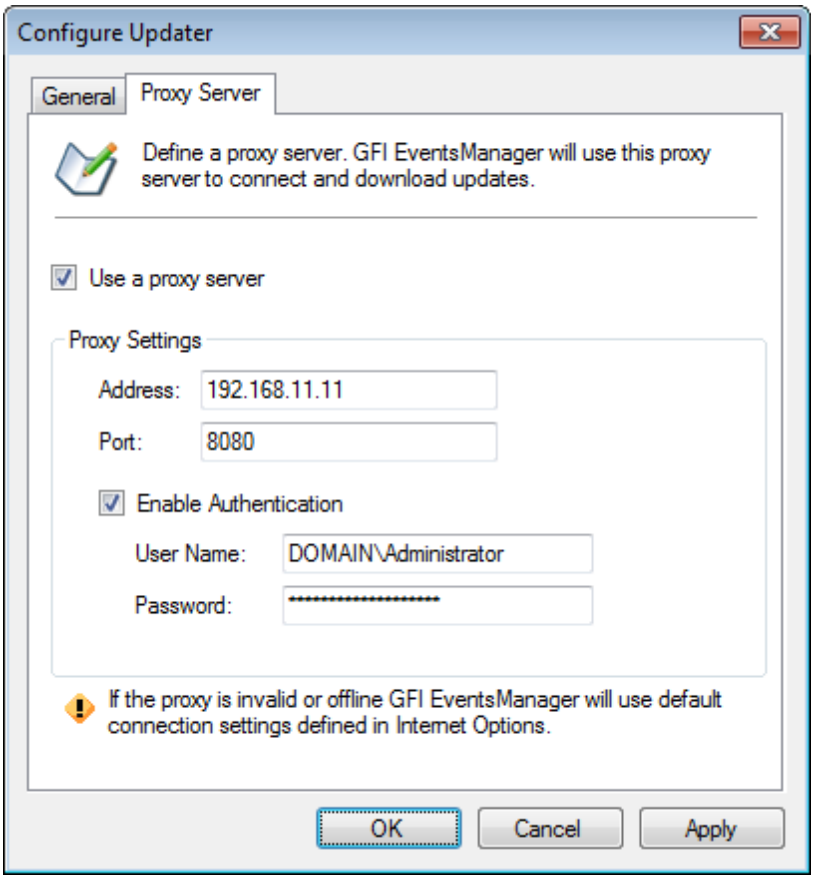
Screenshot 254: Configure auto update options

2. Configure the options described below:

Table 94: Auto update options

Options	Description
Check for updates automatically	If selected, GFI EventsManager will check for updates automatically on a daily or weekly basis.
Update Now	If **Check for updates automatically** is not selected, use this option to manually check for updates and install missing updates.
Install updates automatically	Installs downloaded updates automatically.
Only notify me when updates are available	Available updates are shown in the **Missing Updates** section but are not installed.
Show messages in the application	Shows a message at the bottom of the application page. Click on the displayed message to action the updates.
Send alerts on GFI EventsManager Administrator user	Sends an email alert on the configured GFI EventsManagerAdministrator account. For more information refer to Configuring the administrator account.

3. If product updates must be downloaded through a proxy server, click the **Proxy Server** tab.



Screenshot 255: Configuring proxy settings to download product updates

4. Select **Use a proxy server** and key in the proxy server address and listening port in the **Address** and **Port** fields.

5. (Optional) If the proxy server requires authentication, select **Enable Authentication** and key in the proxy logon credentials.

6. Click **Apply** and **OK**.

15.2.2 Downloading updates from an alternate location (offline)

To download product updates, GFI EventsManager connects to GFI's updates server. If the GFI EventsManager host is in a secure environment, not connected to the Internet, updates can be downloaded from an alternate location.

From a computer with Internet access, download the updates package and transfer it to the GFI EventsManager host. Use CMD to manually launch an update session, using the updater tool provided in the install directory.

You will need a username and password to log into the GFI updates server. To obtain your login credentials, contact one of our support representatives. For more information, refer to Requesting Technical Support.

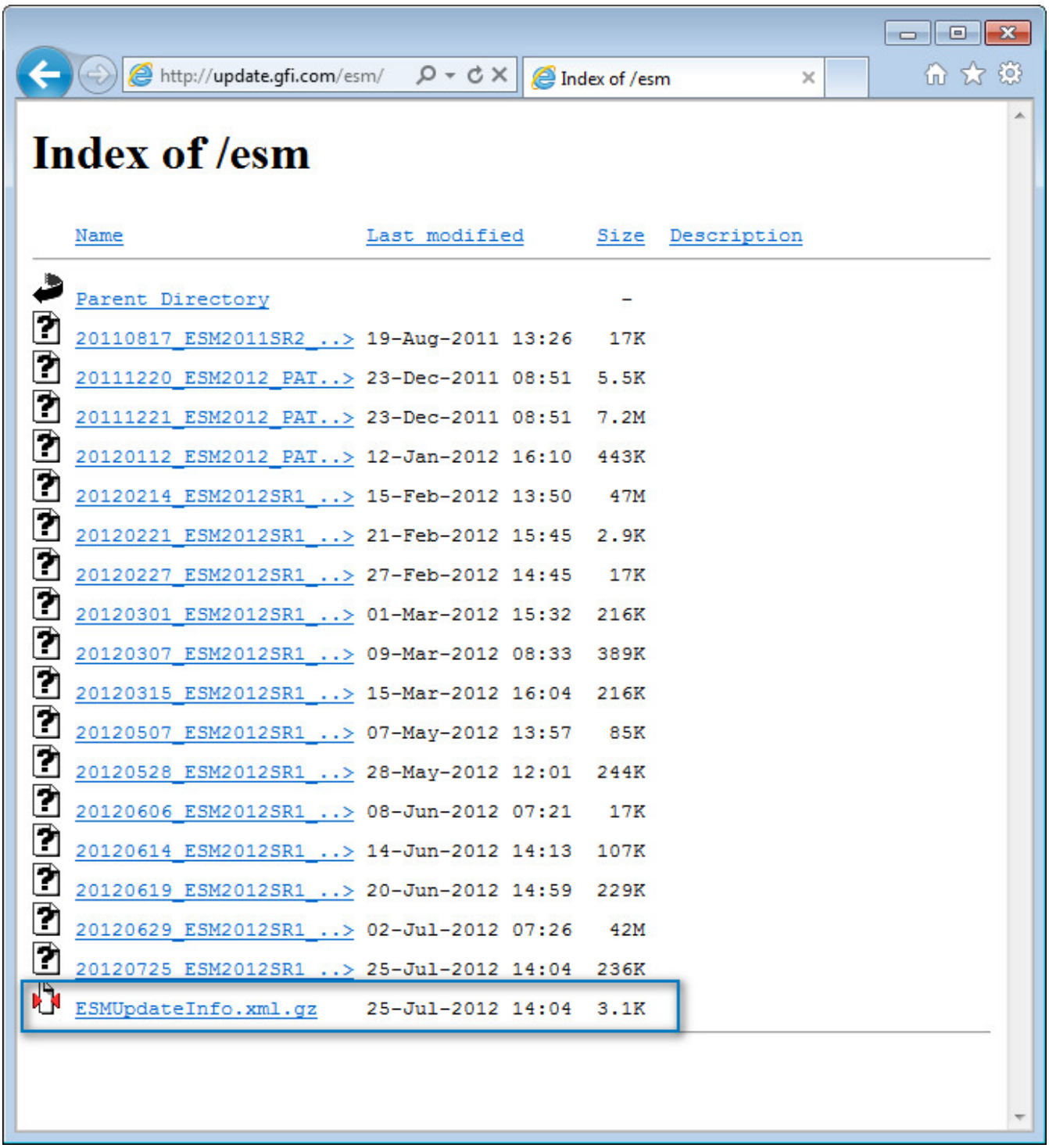
Note

This procedure assumes that the product is installed in the default location: **C:\Program Files (x86)\GFI\EventsManager2012**.

To download updates from an alternate location:

1. On a computer with Internet access, go to http://update.gfi.com/esm.

2. Key in your username and password. This opens the GFI EventsManager updates directory on the updates server.

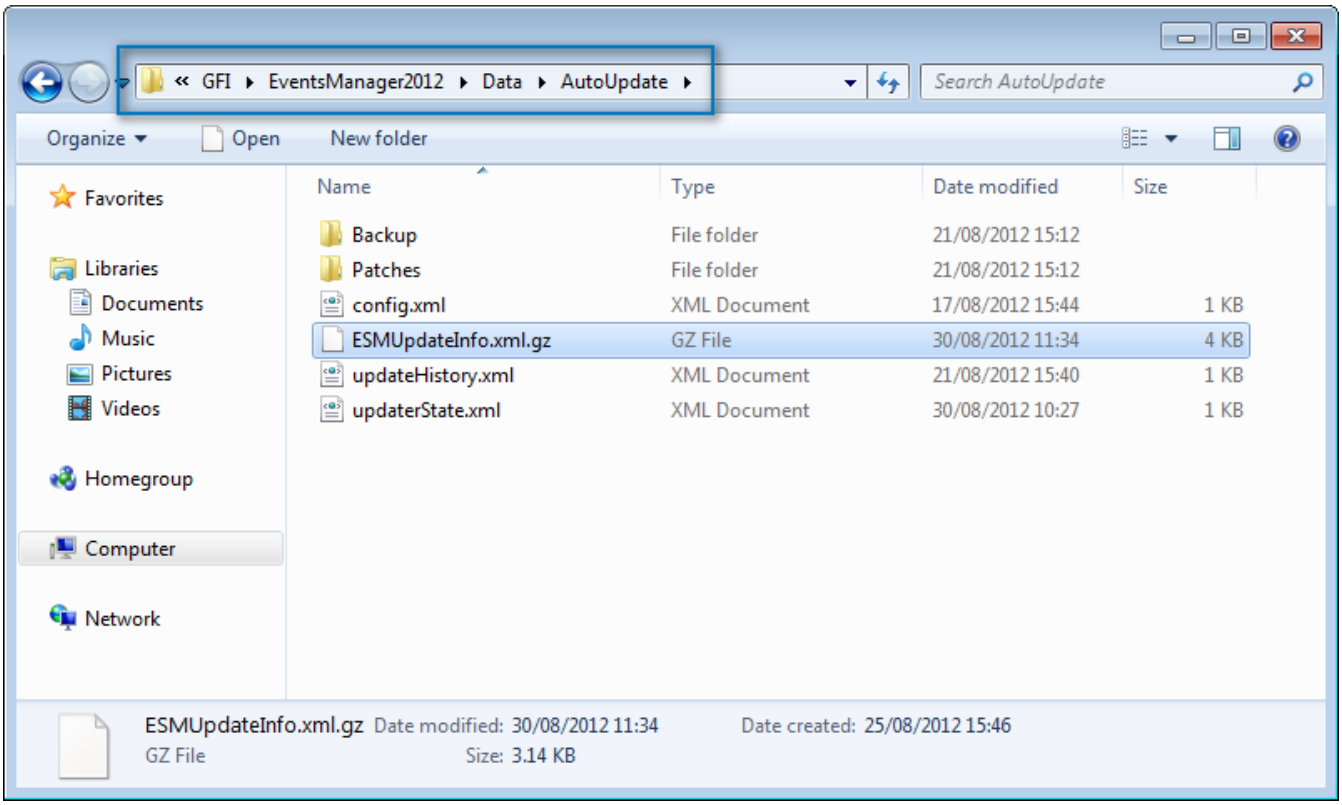


Screenshot 256: GFI EventsManager updates

3. Click **ESMUpdateInfo.xml.gz** and save it to a location of your choice.

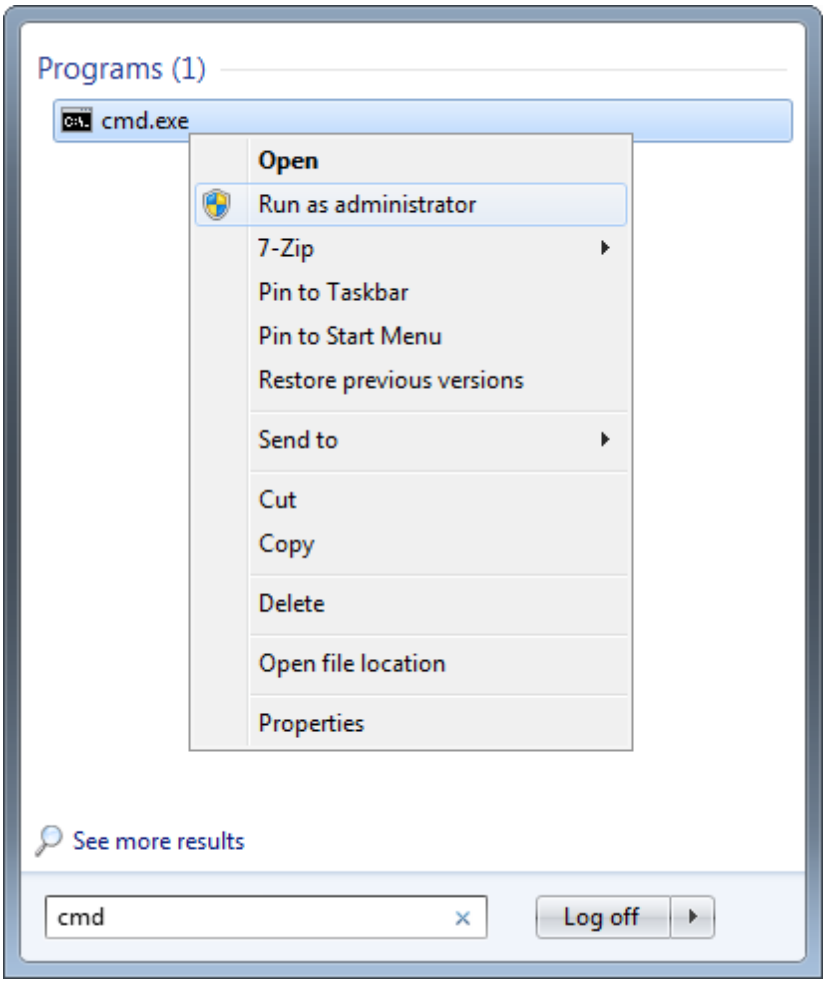
Note

Transfer the downloaded updates package from the computer with Internet access to the GFI EventsManager host.



Screenshot 257: GFI EventsManager updates repository

4. On the GFI EventsManager machine, copy the updates package to the following repository: **C:\Program Files\GFI\EventsManager2012\Data\AutoUpdate**.

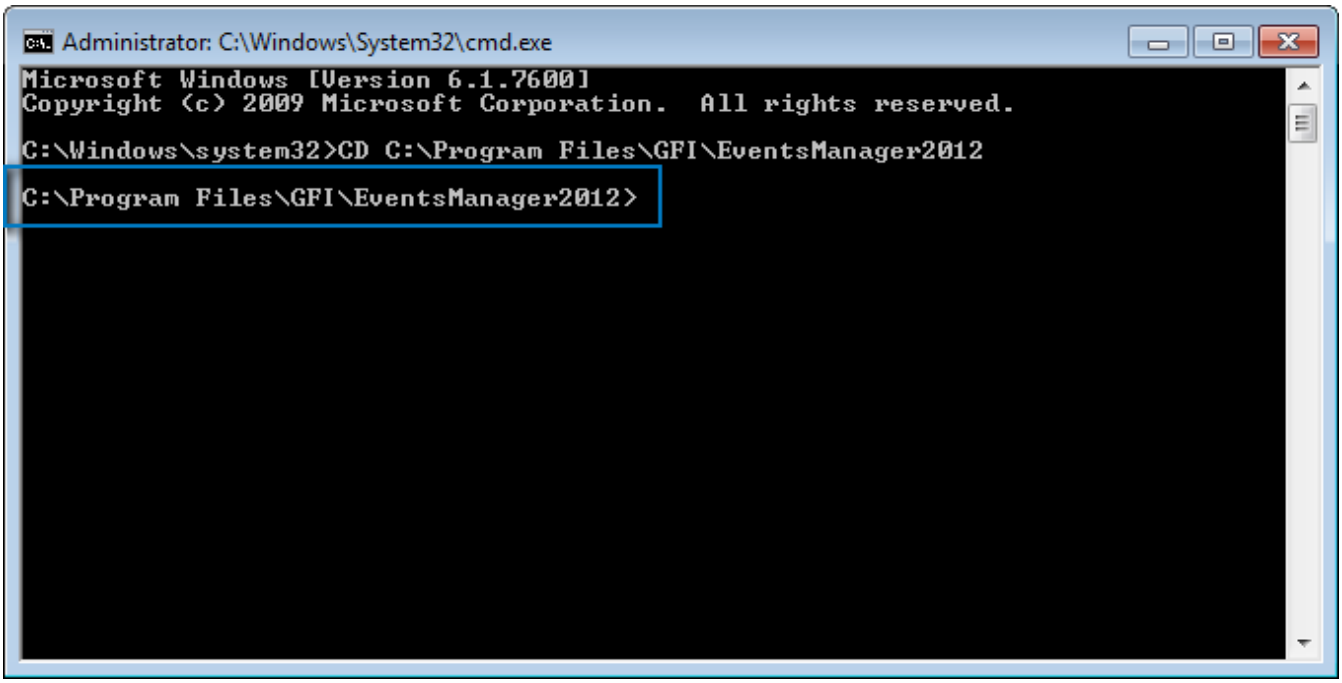


Screenshot 258: Open CMD in administrator mode

5. Open CMD in elevated privileges mode, and key in:

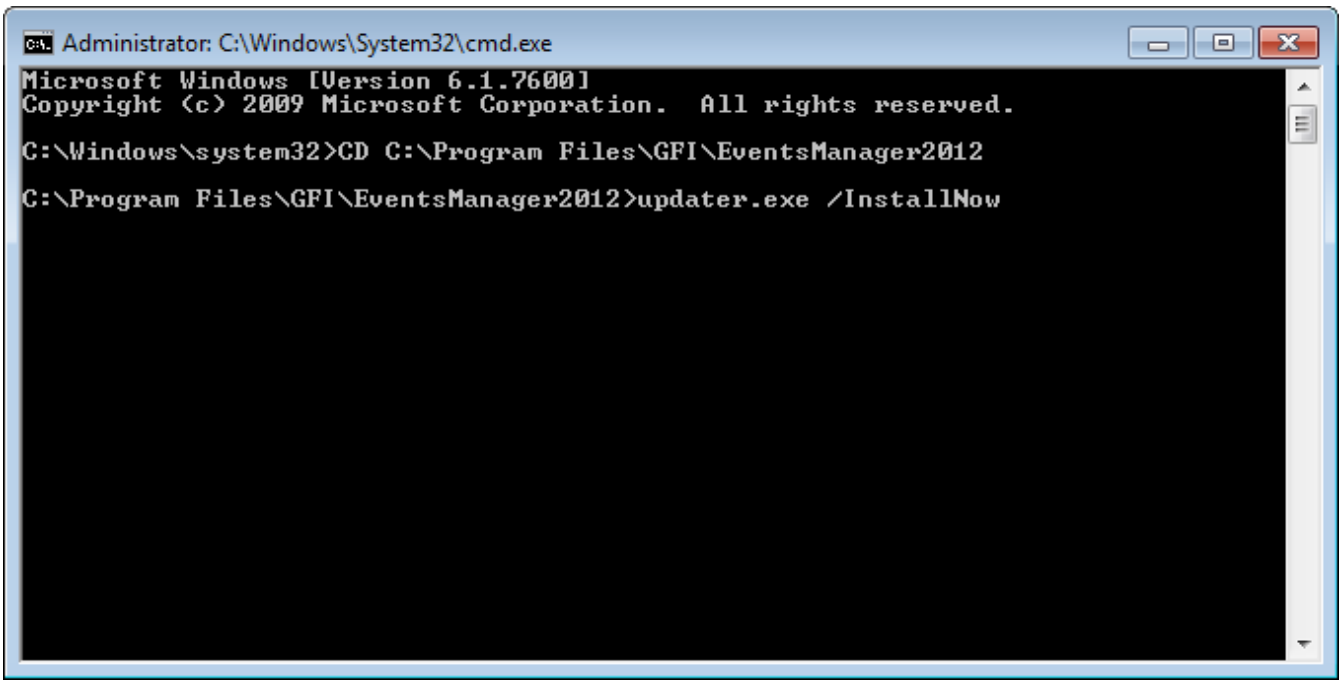
- **64-bit systems** - `CD C:\Program Files (x86)\GFI\EventsManager2012`
- **32-bit systems** - `CD C:\Program Files\GFI\EventsManager2012`

Press **Enter**.



Screenshot 259: Change path to GFI EventsManager install directory

> **Note**
>
> The path changes according to the directory you specify.


Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>CD C:\Program Files\GFI\EventsManager2012
C:\Program Files\GFI\EventsManager2012>updater.exe /InstallNow

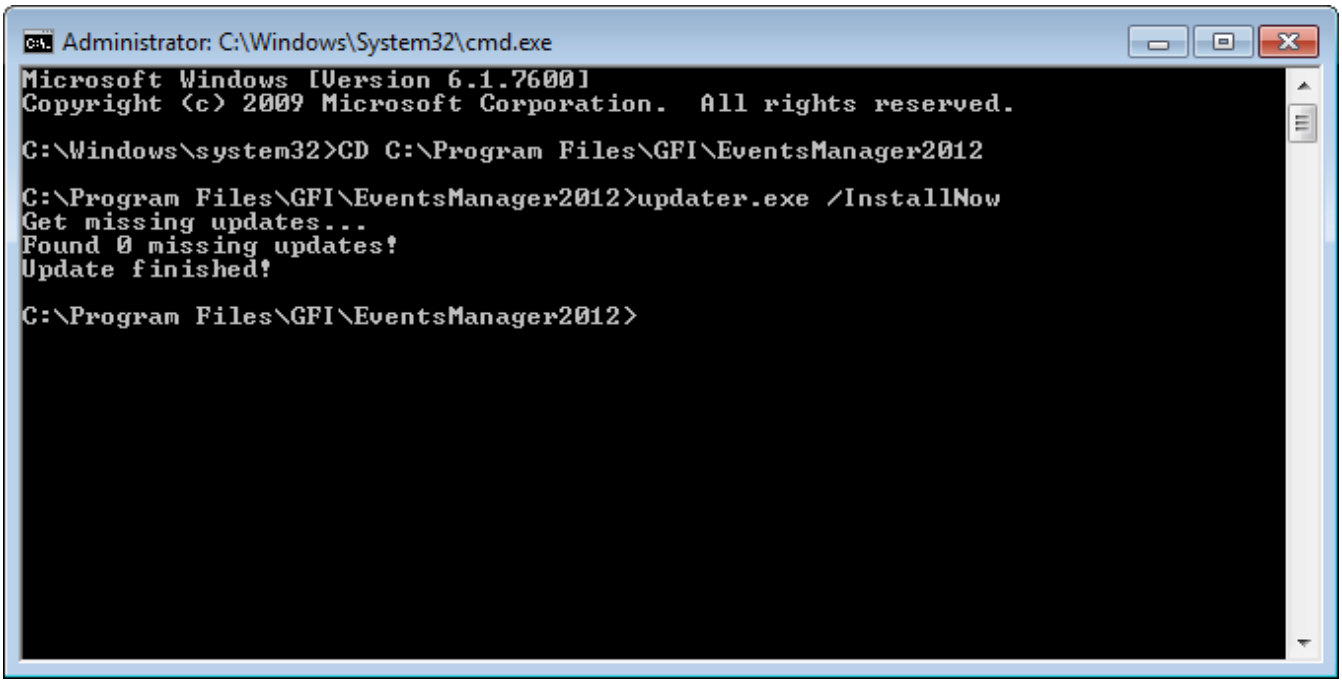
Screenshot 260: Manually launch an update session

6. Key in:

```
updater.exe /InstallNow
```

Press **Enter**.

To ensure that all updates are installed, run `updater.exe /InstallNow`, until you get a message indicating that 0 missing updates were found.



Screenshot 261: Updates status

15.3 Product licensing

GFI EventsManager is licensed by event source/computer. All devices that generate a log are considered to be an event source. Refer to the sections below for more information about GFI EventsManager licensing options.

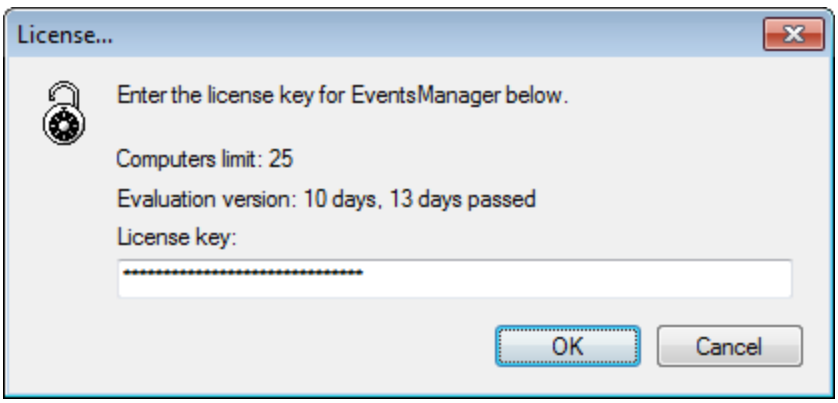
The following sections contain information about:

- Updating license key
- Obtaining a free 30-day trial license key
- Viewing license details
- Purchasing a license key

15.3.1 Updating license key

To update your current license key:

1. From **General** tab > **General**, right-click **Licensing** and select **Update key...**



Screenshot 262: Update license key dialog

3. Specify your license key and click **OK**.

15.3.2 Obtaining a free 30-day trial license key

GFI EventsManager allows you to register your version of the product and receive a free 30-day trial. Once the trial period is expired, all event log monitoring and management services are disabled and a full license key is required.

To register and receive a 30-day trial license key:

1. From **General** tab > **General**, click **Licensing**.

2. Click the provided link. This will take you to GFI website where you are able to enter you details and receive the license key by email. The email address you provide in the registration form is where your free 30-day trial key will be sent. If you have a spam filtering system, make sure the email is not blocked as spam.

15.3.3 Viewing license details

License details provide you with license distribution details. To view licensing details:

1. From **General** tab > **General**, click **Licensing**.

2. From the right pane, click **Show details** to expand the details section. This will show the number of event sources configured and respective license type (such as Workstation or Server).

15.3.4 Purchasing a license key

To purchase a license key:

1. From **General** tab > **General**, click **Licensing**.

Screenshot 263: Buy now! Button

2. From the right pane, click **Buy now!**. This takes you to GFI website where you can view further information about licensing and purchase a valid key.

Note

For more information, refer to:

- Licensing Information - http://www.gfi.com/page/13789/products/gfi-events-manager/pricing/licensing/licensing
- Pricing Information - http://www.gfi.com/products/gfi-eventsmanager/pricing

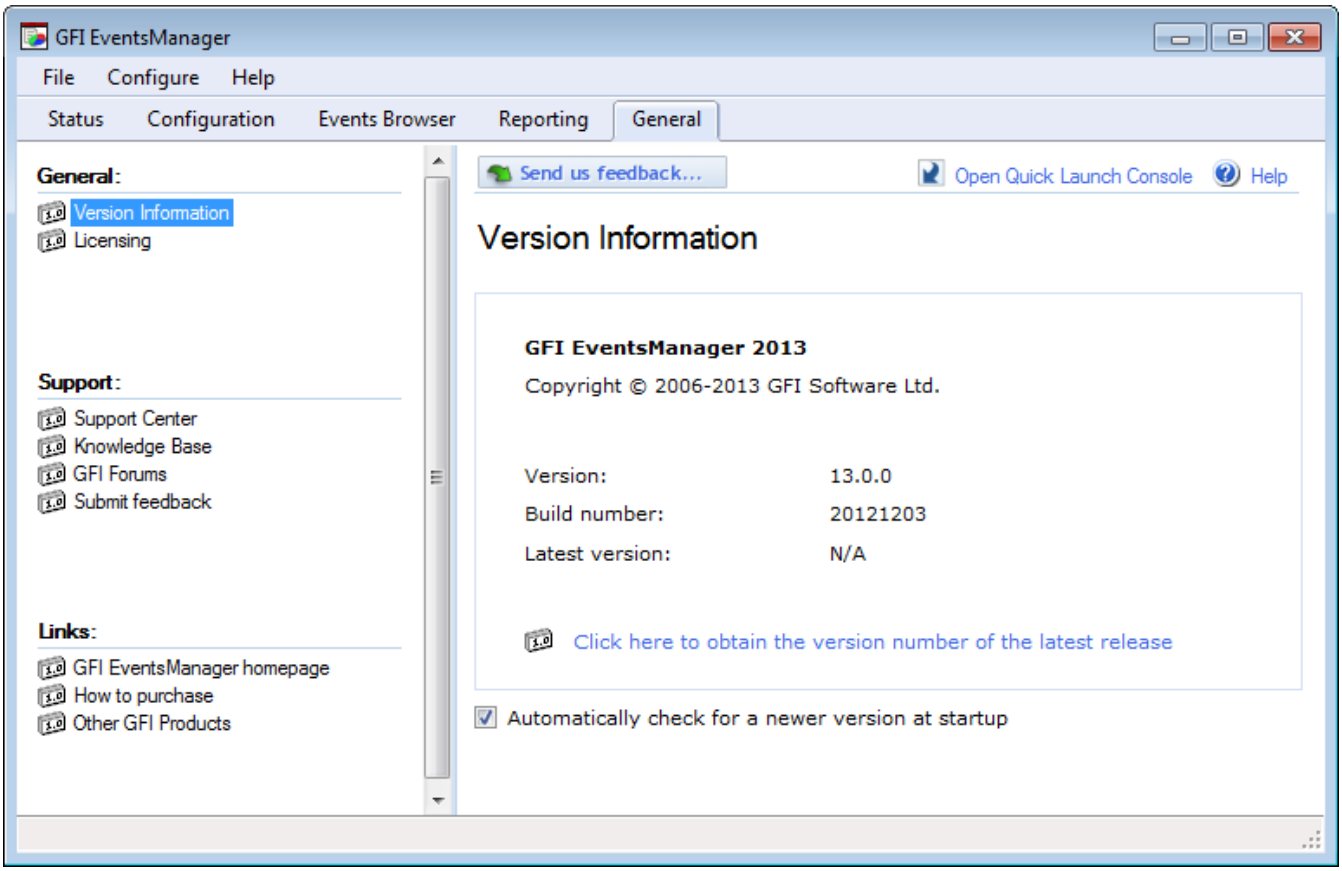
15.4 Product version information

GFI recommends that you keep GFI EventsManager up-to-date and use the latest product version for full feature support and device compatibility. Version information can also be useful to troubleshoot functionality errors with a technical support representative. Refer to the following sections for information about:

15.4.1 Checking your GFI EventsManager version

To check your version information details:

1. From **General** tab > **General**, click **Version Information**.



Screenshot 264: Version Information screen

2. View version information details from the right pane.

3. (Optional) Click **Click here to obtain the version number of the latest release** to get the latest version information from GFI servers.

15.4.2 Checking for newer versions

To check for newer builds of GFI EventsManager:

1. From **General** tab > **General**, right-click **Version Information** and select **Check for newer builds...**

2. (Optional) From the right pane, select/unselect **Automatically check for a newer version at startup** to check for new versions automatically. By default, this option is enabled.

15.5 Importing and Exporting settings

The provided import and export tool, enables you to seamlessly move configurations from one instance of GFI EventsManager to another. This can also be done as part of a disaster recovery plan, to avoid having to reconfigure GFI EventsManager in case of a disaster. The following settings can be imported/exported using GFI EventsManager:

- Event Sources
- Event Processing Rules
- Events Browser Filters
- Options (including Default Classification Actions, Alerting Options, Database operations and more).

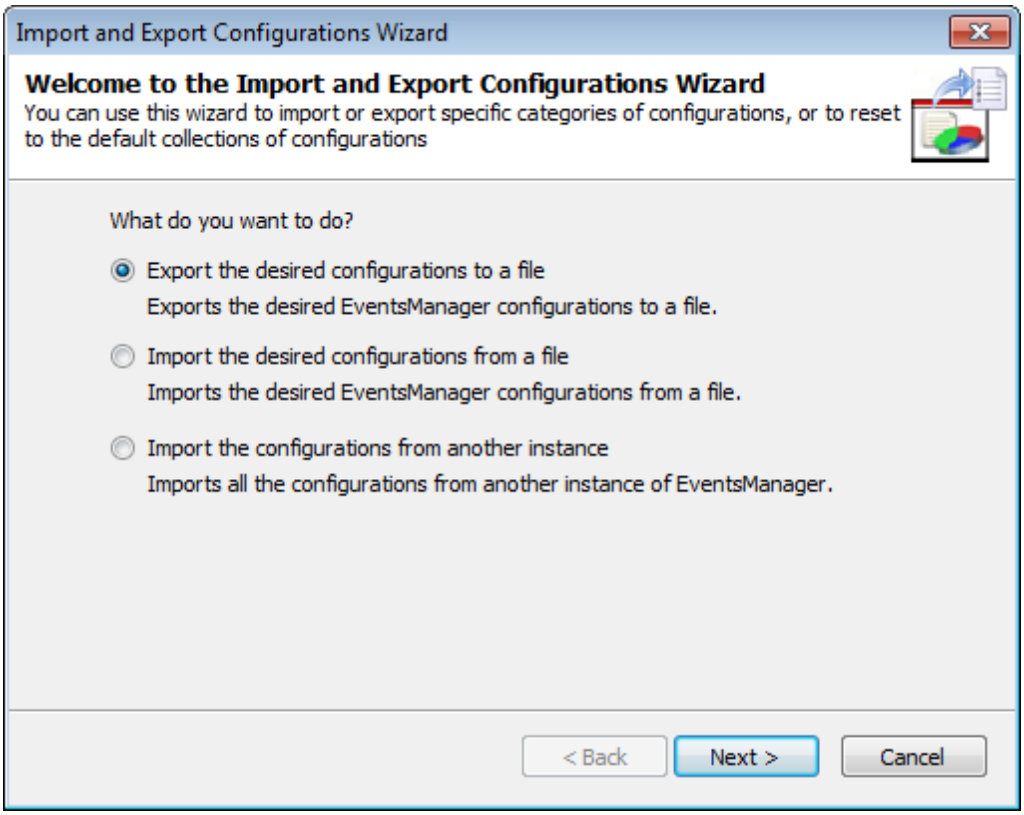
This section contains information about:

- Exporting configurations to a file
- Importing configurations from a file
- Importing configurations from another instance

15.5.1 Exporting configurations to a file

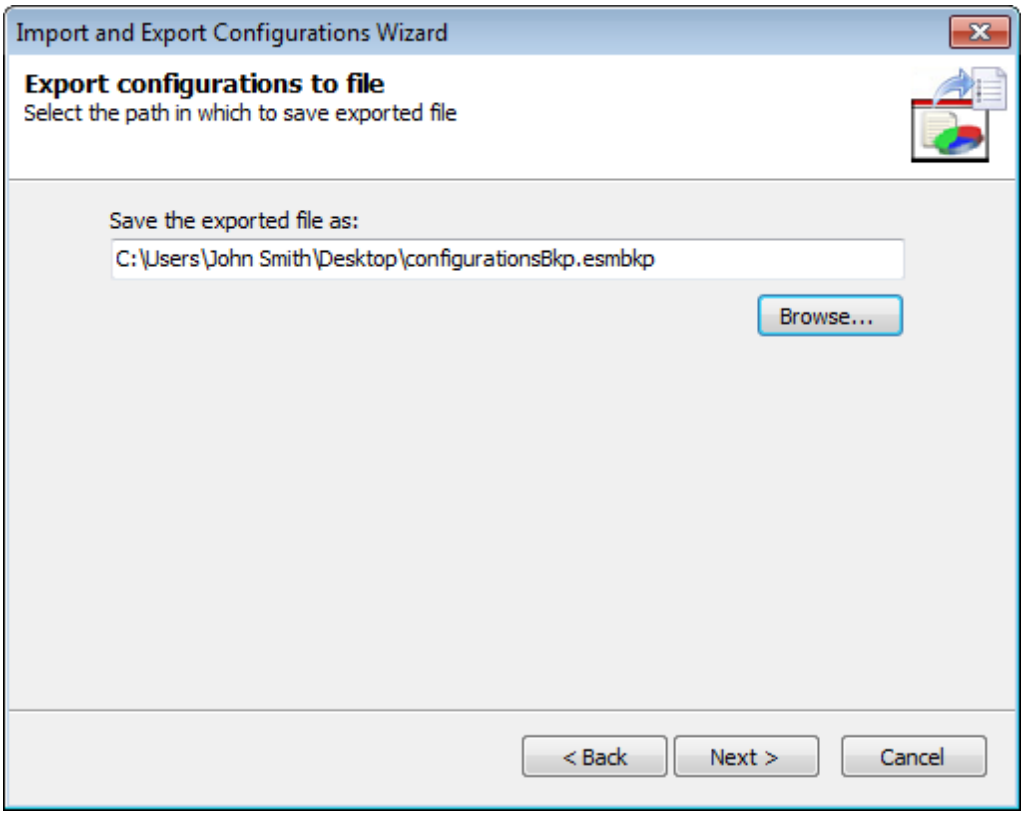
To export you GFI EventsManager configurations:

1. Click **File > Import and Export Configurations...**.


Import and Export Configurations Wizard
Welcome to the Import and Export Configurations Wizard
You can use this wizard to import or export specific categories of configurations, or to reset to the default collections of configurations
What do you want to do?
Export the desired configurations to a file
Exports the desired EventsManager configurations to a file.
Import the desired configurations from a file
Imports the desired EventsManager configurations from a file.
Import the configurations from another instance
Imports all the configurations from another instance of EventsManager.
< Back
Next >
Cancel

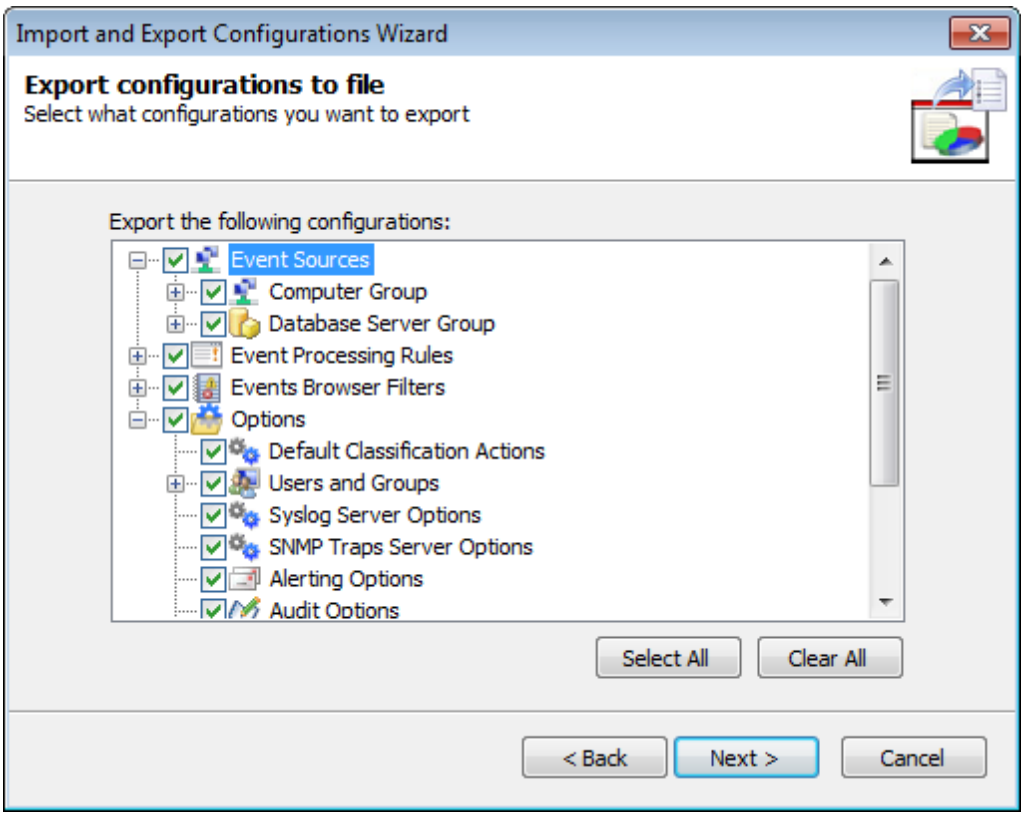
Screenshot 265: Export configurations to a file

2. Select **Export the desired configurations to a file** and click **Next**.



Screenshot 266: Specify export destination

3. Specify the location where the exported file will be saved or click **Browse...** to look for the location. Click **Next**.



Screenshot 267: Select export configurations

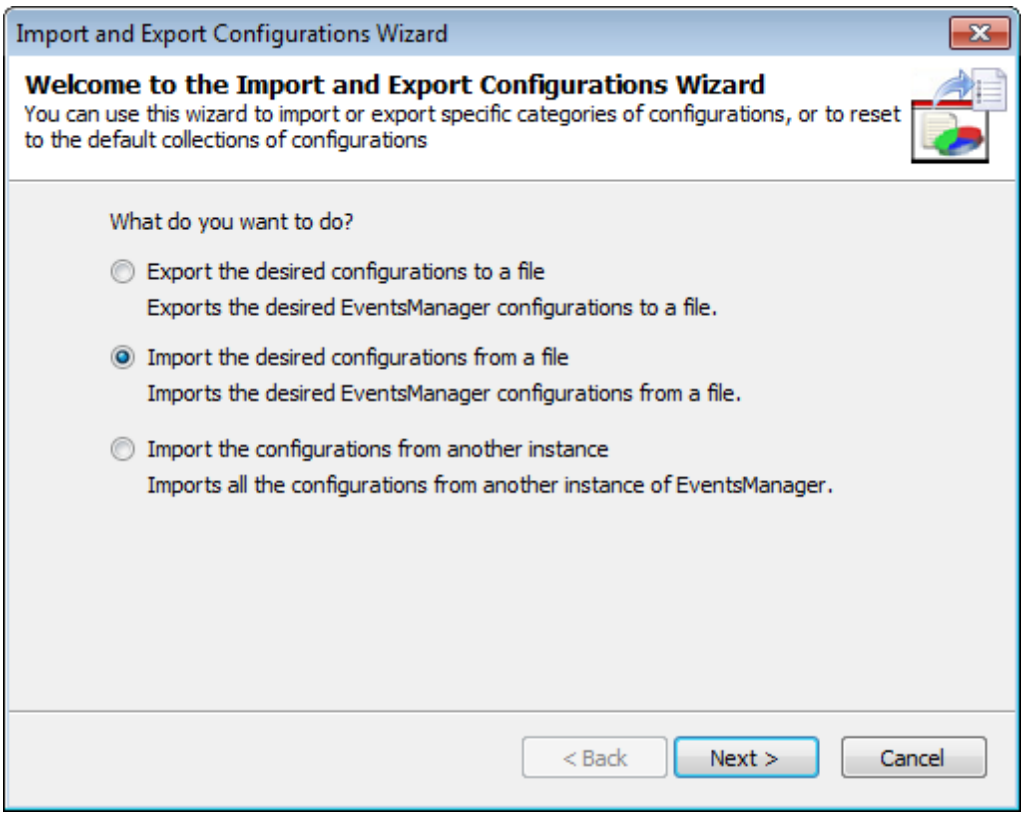
4. Select the configurations you want to export and click **Next**.

5. Wait for GFI EventsManager to export the configuration and click **OK**.

15.5.2 Importing configurations from a file

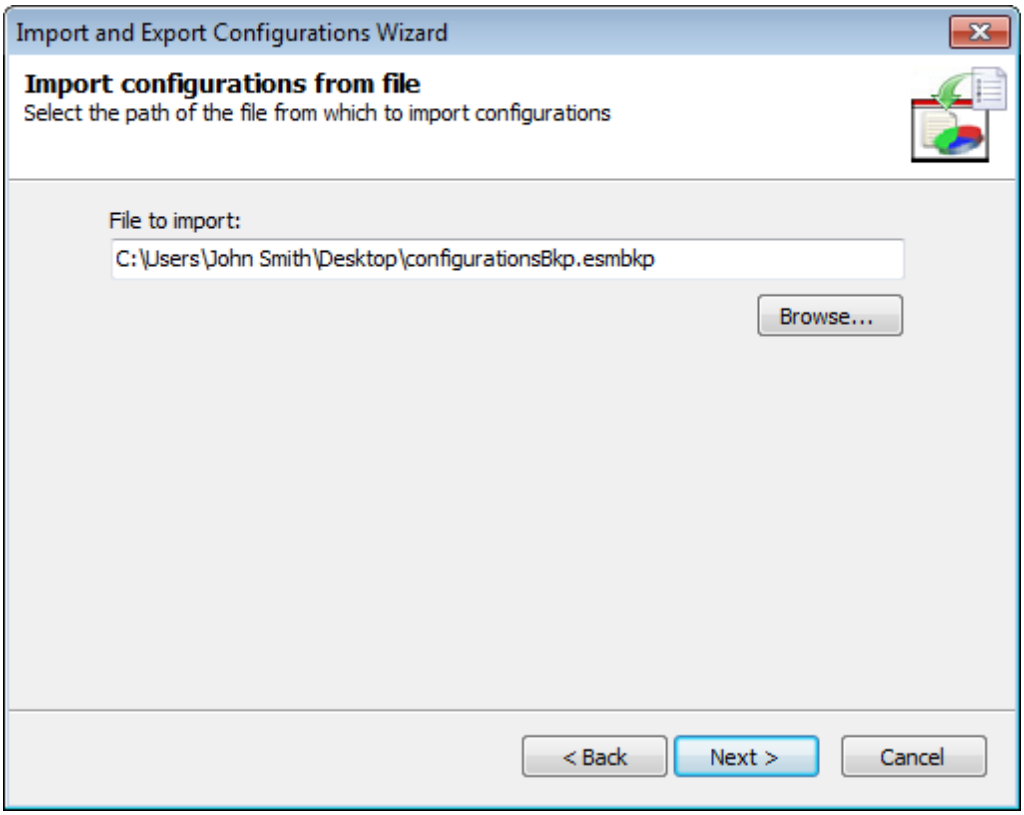
To import configurations from a file:

1. Click **File > Import and Export Configurations....**


Import and Export Configurations Wizard
Welcome to the Import and Export Configurations Wizard
You can use this wizard to import or export specific categories of configurations, or to reset to the default collections of configurations
What do you want to do?
Export the desired configurations to a file
Exports the desired EventsManager configurations to a file.
Import the desired configurations from a file
Imports the desired EventsManager configurations from a file.
Import the configurations from another instance
Imports all the configurations from another instance of EventsManager.
< Back
Next >
Cancel

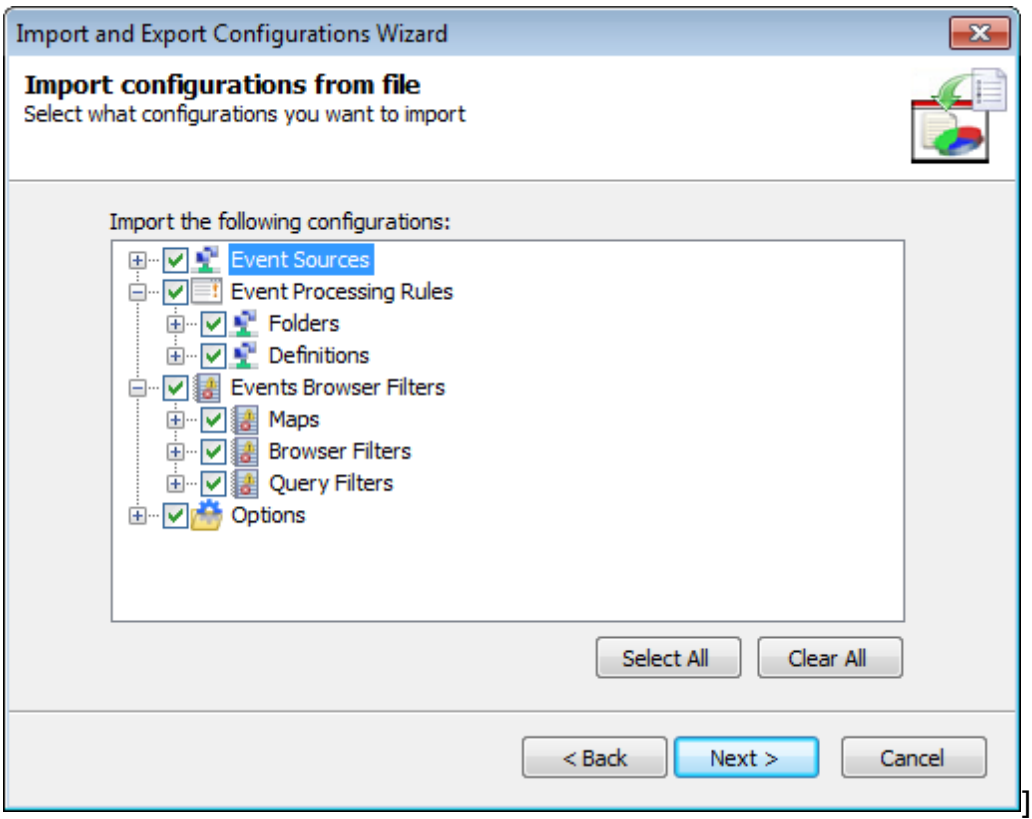
Screenshot 268: Import configurations from a file

2. Select **Import the desired configurations from a file** and click **Next**.



Screenshot 269: Specify configuration file location

3. Specify the path where the import file is stored or click **Browse...** to look for it. Click **Next**.



Screenshot 270: Select configurations to import

4. Select the configurations you want to import and click **Next**.

5. Wait for GFI EventsManager to import the configurations and click **OK**.

Note

If GFI EventsManager detects other configurations, it will ask you if you want to override or merge both configurations.

15.5.3 Importing configurations from another instance

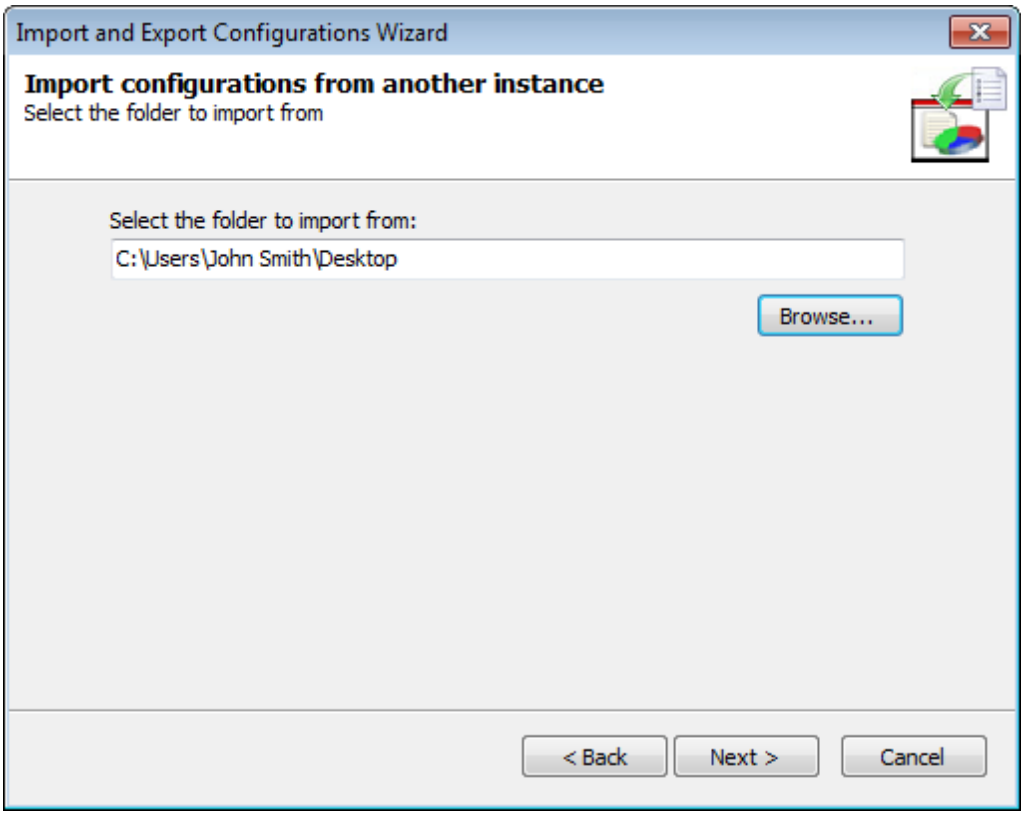
To import configurations from another instance of GFI EventsManager:

1. Click **File > Import and Export Configurations...**

Import and Export Configurations Wizard
Welcome to the Import and Export Configurations Wizard
You can use this wizard to import or export specific categories of configurations, or to reset to the default collections of configurations
What do you want to do?
Export the desired configurations to a file
Exports the desired EventsManager configurations to a file.
Import the desired configurations from a file
Imports the desired EventsManager configurations from a file.
Import the configurations from another instance
Imports all the configurations from another instance of EventsManager.
< Back
Next >
Cancel

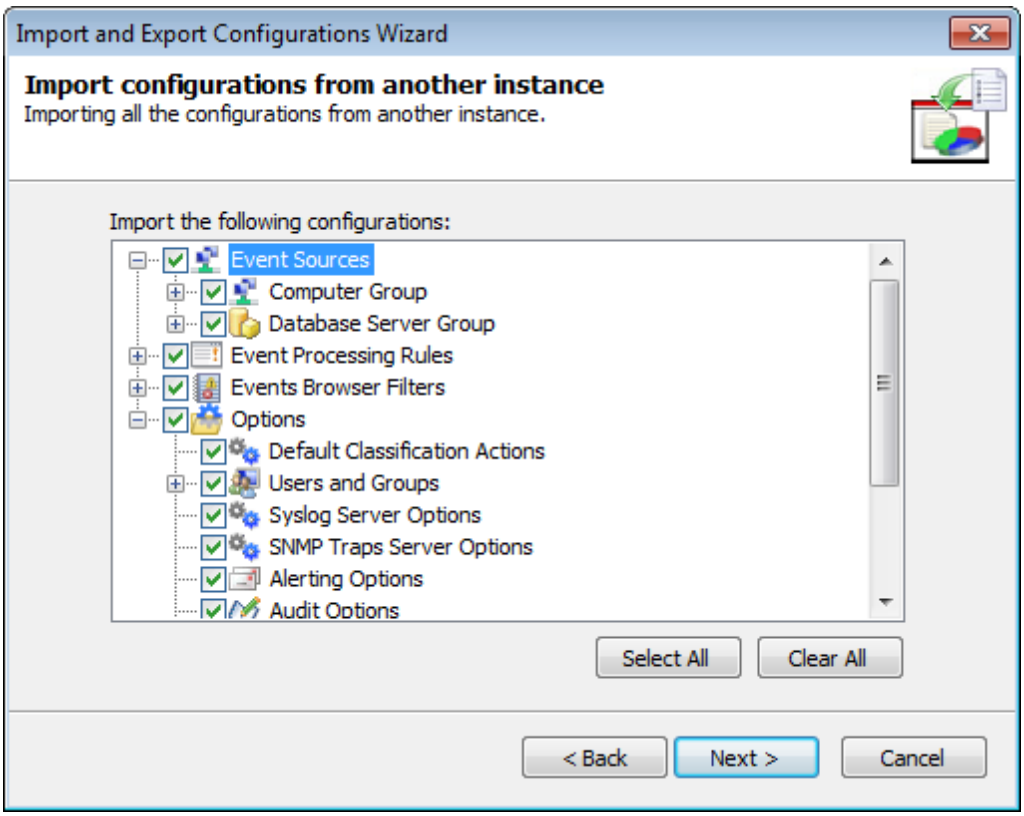
Screenshot 271: Import configurations from another instance of GFI EventsManager

2. Select **Import the configurations from another instance** and click **Next**.



Screenshot 272: Specify instance location

3. Specify the installation folder path of the instance you want to import configurations from. Alternatively, click **Browse...** to look for it. Click **Next**.



Screenshot 273: Select configurations to import from another instance of GFI EventsManager

4. Select the configurations you want to import and click **Next**.

5. Wait for the configurations to import and click **OK**.

> **Note**
>
> If GFI EventsManager detects other configurations, it will ask you if you want to override or merge both configurations.

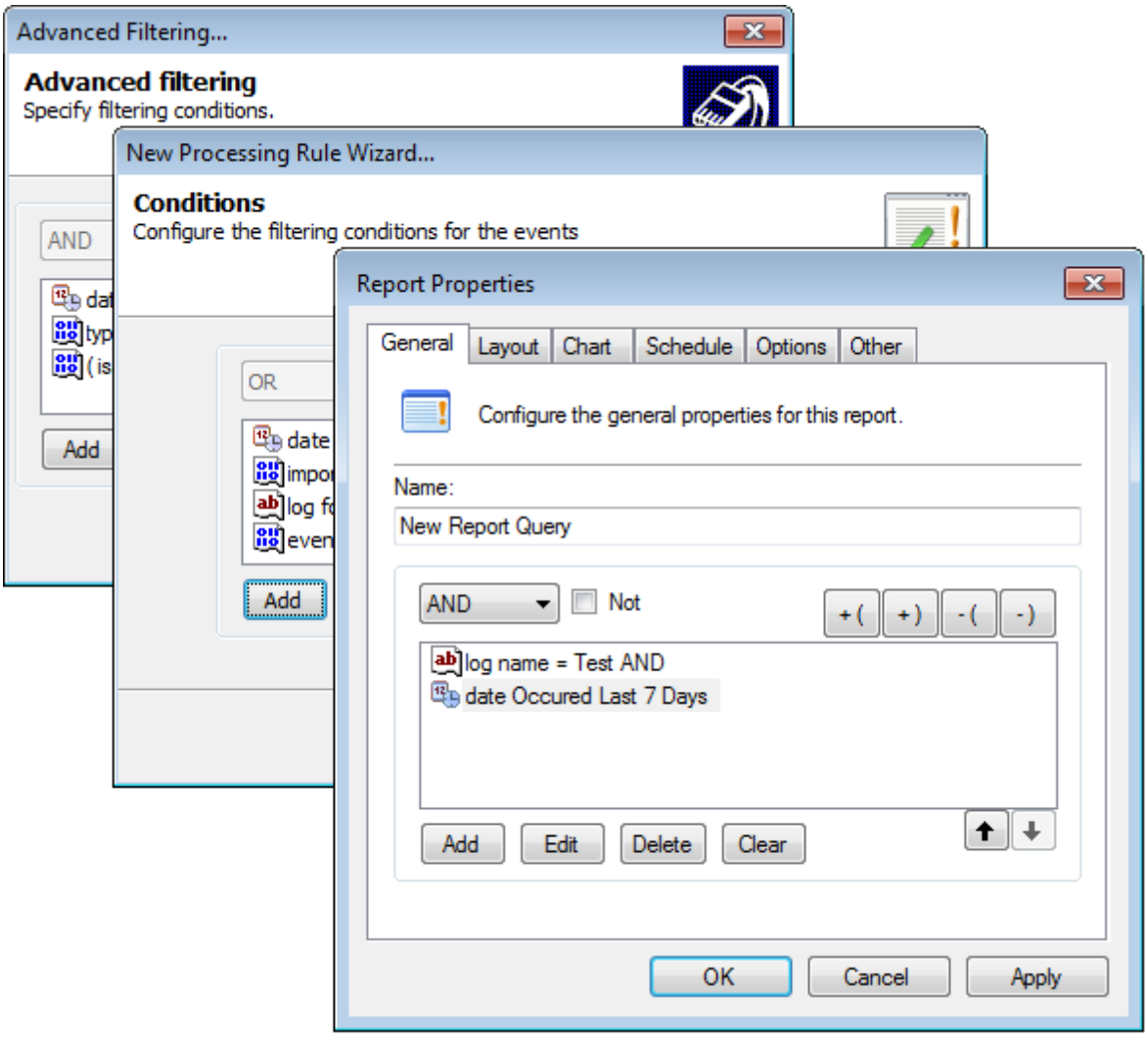
15.6 Building query restrictions

GFI EventsManager enables you to build custom queries, using the **Edit Query Restriction** dialog. Queries are instructions GFI EventsManager sends to the database backend when storing and retrieving data. They are also used to configure rules to trigger actions and alerts when certain attribute values are detected.

The following scenarios use the Edit Query Restriction dialog for granular configuration:

Table 95: Uses of query restrictions

Use	Description
Configuring reports	Build queries to filter report information and generate reports pertaining to specific attributes.
Configuring user accounts	Prevent GFI EventsManager Management Console users from displaying unauthorized information about other users, event logs or network activity.
Configuring events processing rules	Scan collected event logs for attributes that match values configured in events processing queries. This enables you to inspect network activity in granular detail, which helps you to proactively resolve network issues before evolving into serious problems.



Screenshot 274: Users, Events processing rules and Report queries

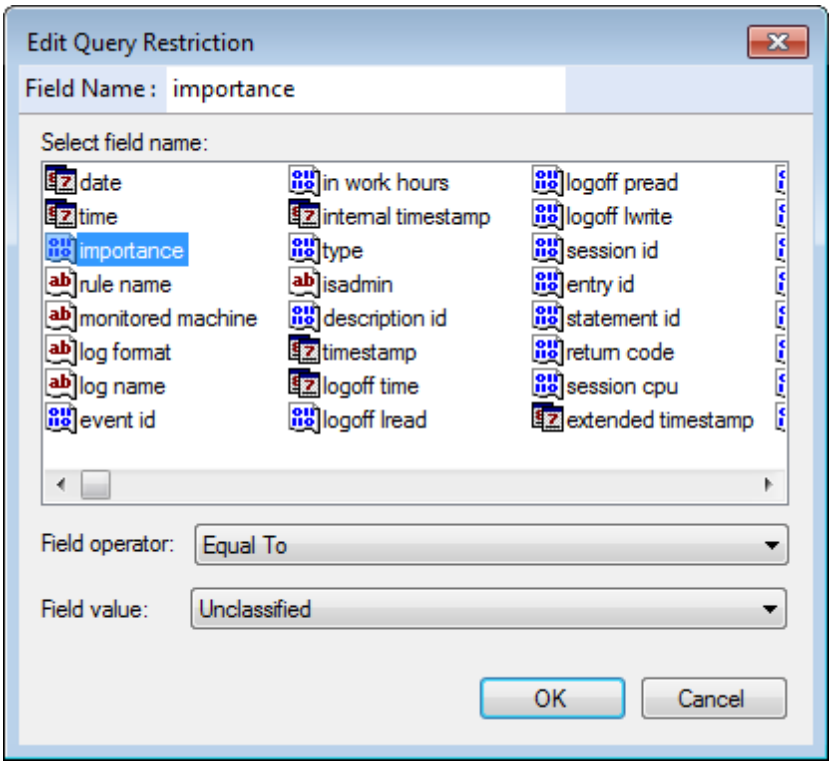
15.6.1 Using the Edit Query Restriction dialog

To edit query restrictions for granular filtering and configuration:

1. The following table describes how to launch the Edit Query Restriction dialog for users, reports and processing rules:

Table 96: Launching the Edit Query Restrictions dialog

Configure...	Procedure
Users	To launch the query restrictions dialog: 1. Click **Configuration** tab > **Options** > **Users and Groups** > **Users**. 2. From the right-pane, right-click the user to edit and select **Properties**. 3. From the **User Properties** dialog, click **Filter** tab > **Advanced...** 4. From the **Advanced filtering** dialog, click **Add**.
Reports	To launch the query restrictions dialog: 1. Click **Reporting** tab. 2. From the **Reports** list, right-click the report to edit and select **Properties**. 3. From the **General** tab, click **Add**.
Events processing rules	To launch the query restrictions dialog: 1. Click **Configuration** tab > **Events Processing Rules**. 2. From the **Rule Folders** list, right-click the events processing rule to edit and select **Properties**. 3. From the processing rule properties dialog, click **Conditions** tab > **Add**.



Screenshot 275: Defining restrictions: Editing a query restriction

2. From the list of available fields, select a field. Optionally, key in the name in **Field Name** text box to search for the required field.

3. Specify a **Field Operator** for the selected field. Available operators include:

Table 97: Defining restrictions: Field Operators

Field Operator	Description
Equal To	When the event field is equal to the value configured.
Less than	When the event field is has a smaller value than the value configured.
Greater than	When the event field is has a larger value than the value configured.
Occurred (Related to date/time fields)	When the event field date occurred before the value date.
Like	When the event field has similar text as the value text.
Contains	When the event field contains the value text.
Value in List	When the event field is equal to one of the values in a list.

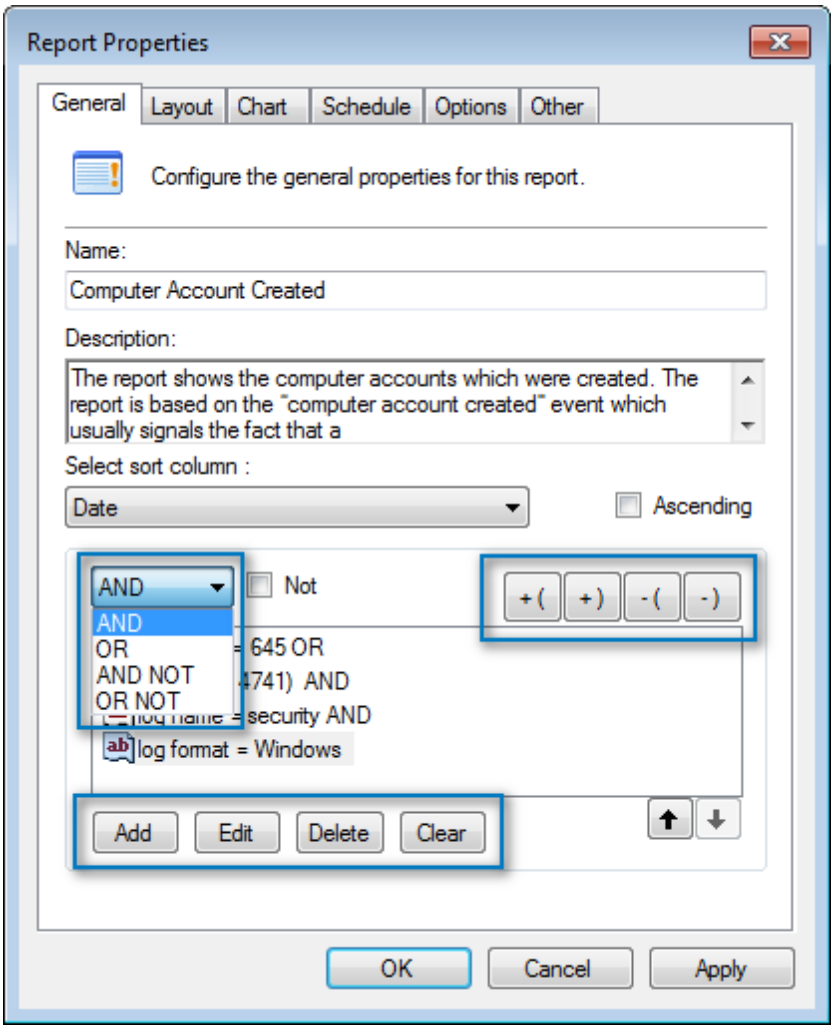
4. Specify a **Field Value** for the selected field and operator. Some fields have predefined values; others require you to specify a value.

5. Click **OK**.

> **Note**
>
> Repeat steps 1 to 4 to add all the fields you want to include in the query.

Note

You can copy report restrictions from existing reports. From **Reporting** tab > **Reports**, right-click a report and select **Copy Report Restrictions**.



Screenshot 276: Defining restrictions: Customizing the condition

6. Once all the restrictions are defined, use the options described below to customize the query conditions:

Table 98: Defining restrictions: Query Condition tools

Options	Description
AND	Select the condition to configure and select AND. The selected condition AND the following condition(s) must be met for the query to be valid.
OR	Select the condition to configure and select OR. The selected condition OR the following condition(s) must be met for the query to be valid.
AND NOT	Select the condition to configure and select AND NOT. This means that the selected condition has to match the restriction parameters but the following conditions must not.
OR NOT	Select the condition to configure and select OR NOT. This means that the selected condition has to match the restriction parameters OR the following conditions must not.
+ (	Click '+ (' to add an opening bracket to the selected condition. Conditions enclosed in brackets are processed first.

Options	Description
+)	Click '+)' to add a closing bracket to the selected condition. Conditions enclosed in brackets are processed first.
- (	Click '- (' to remove an opening bracket from the selected condition.
-)	Click '-)' to remove a closing bracket from the selected condition.
Add	Click Add to launch the restrictions dialog and add more fields to the condition.
Edit	Click Edit to access the restrictions dialog and customize the selected condition.
Delete	Click Delete to delete a condition.
Clear	The Clear button deletes all the query conditions.
Up arrow	Use the Up arrow key to move the selected condition up in the list.
Down arrow	Use the Down arrow key to move the selected condition down in the list.

7. Click **Apply** and **OK**.

16 Command Line Tools

GFI EventsManager provides you with command line tools through which you can perform various functions without accessing the Management Console. The available CMD tools are located in the GFI EventsManager install folder.

Topics in this chapter:

16.1 Using ESMCmdConfig.exe 307

16.2 Using EsmDlibM.exe 310

16.3 Using DLibAdm.exe 318

16.4 Using EsmReport.exe 320

16.1 Using ESMCmdConfig.exe

ESMCmdConfig.exe enables you to configure general settings for GFI EventsManager; such as:

- GFI EventsManager logon credentials
- License key
- Mail server settings
- Administrator account
- Create/Remove Group shortcuts
- Get computer names.

To use ESMCmdConfig.exe:

1. Click **Start > Run** and key in **CMD**.
2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.
3. Change the directory to the GFI EventsManager install directory. Example:

```
CD <C:\Program Files\GFI\EventsManager>
```

4. Key in **ESMCmdConfig.exe** followed by the functions described below:

- /op:registerService
- /op:enable
- /op:disable
- /op:SetLicense
- /op:configureAlerting
- /op:setAdminEmail
- /op:createProgramGroupShortcuts
- /op:removeProgramGroupShortcuts
- /op:getComputers

16.1.1 /op:registerService

This function enables you to register GFI EventsManager services, using an administrator account. The following parameters are supported:

Table 99: /op:registerService Parameters

Parameter	Description
/username:<*username*>	Specify the username of an administrator account. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/pass:<*password*>	Specify the password for the account specified in the **/username** parameter.

Example

```
ESMCmdConfig.exe /op:registerService /username:Domain\Administrator
/pass:p@ss
```

16.1.2 /op:enable

This function enables you to turn on events management features and does not support additional parameters.

Example

```
ESMCmdConfig.exe /op:enable
```

16.1.3 /op:disable

This function enables you to turn off events management features and prompts the user with a custom message. The following parameter is supported:

Table 100: /op:disable Parameter

Parameter	Description
/message:<*message*>	Specify a custom message that is shown to the user before events management features are disabled. **Note** Parameters that contain spaces must be enclosed in double quotes (“).

Example

```
ESMCmdConfig.exe /op:disable /message:"Events Management Disabled!"
```

16.1.4 /op:SetLicense

This function enables you to enter the product license key. The following parameter is supported:

Table 101: /op:SetLicense Parameters

Parameter	Description
/licenseKey:<*key*>	Specify the product license key.

Example

```
ESMCmdConfig.exe /op:SetLicense /licenseKey:*********
```

16.1.5 /op:configureAlerting

This function enables you to turn on and configure email alerting options. The following parameters are supported:

Table 102: /op:configureAlerting Parameters

Parameter	Description
/Server:<*server*>	Specify the mail server IP address or fully qualified domain name (FQDN).
/SenderEmail:<*email*>	Specify the sender email address. Notifications appear to have been sent from the specified address.
/Port:<*port*>	Specify the TCP port used to send emails.
/RequiresAuthentication: <*true*|*false*>	Specify if the mail server requires authentication. Supported values are: » True » False.
/User:<*username*>	Specify the username of the email address specified in the **/SenderEmail** parameter. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/Pass:<*password*>	Specify the password for the username specified in the **/User** parameter.

Example

```
ESMCmdConfig.exe /op:configureAlerting /Server:192.168.11.11
/SenderEmail:jsmith@domain.com /Port:25 /RequiresAuthentication:True
/User:jsmith /Pass:p@ss
```

16.1.6 /op:setAdminEmail

This function enables you to configure the EventsManagerAdministrator email address. The following parameter is supported:

Table 103: /op:setAdminEmail Parameter

Parameter	Description
/email:<*email*>	Specify the EventsManagerAdministrator email address.

Example

```
ESMCmdConfig.exe /op:setAdminEmail /email:esmadmin@domain.com
```

16.1.7 /op:createProgramGroupShortcuts

This function enables you to create group shortcuts and has no additional parameters.

Example

```
ESMCmdConfig.exe /op:createProgramGroupShortcuts
```

16.1.8 /op:removeProgramGroupShortcuts

This function enables you to remove group shortcuts and has no additional parameters.

Example

```
ESMCmdConfig.exe /op:removeProgramGroupShortcuts
```

16.1.9 /op:getComputers

This function enables you to retrieve a text file containing the names of event sources managed by GFI EventsManager. The following parameter is supported:

Table 104: /op:getComputers Parameter

Parameter	Description
/filename:<*fileName*>	Specify the full path where the text file is exported to including the name of the text file. **Note** Parameters that contain spaces must be enclosed in double quotes (“).

Example

```
ESMCmdConfig.exe /op:getComputers /filename:C:\ComputerNames.txt
```

16.2 Using EsmDlibM.exe

EsmDlibM.exe enables you to run operations against the file storage system where processed events are stored (database backend). Such operations include Importing or Exporting data.

To use EsmDlibM.exe:

1. Click **Start > Run** and key in **CMD**.
2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.
3. Change the directory to the GFI EventsManager install directory. Example:

```
CD <C:\Program Files\GFI\EventsManager>
```

4. Key in **EsmDlibM.exe** followed by the functions described below:

- /importFromSQL
- /importFromDlib
- /copyData
- /importFromLegacyFile
- /exportToFile
- /importFromFile

- /commitDeletedRecords
- /exportToSQL

16.2.1 /importFromSQL

This function enables you to import data from an SQL Server® database. The data must be exported from an older version of GFI EventsManager. The following parameters are supported:

Table 105: /importFromSQL Parameters

Parameter	Description
/server:<*serverName*>	Specify the SQL Server® IP address or machine name.
/database:<*(maindb)|(backupdb)|databaseName*>	Specify the type and name of the source database to import data from . **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/dbauth:<*SQL|WIN*>	Specify the authentication mode configured in the source SQL Server®. Supported values include: » **SQL**: to use SQL Server® authentication » **WIN**: to use Windows® authentication.
/username:<*username*>	Specify a username that has access to the database from which you want to import data. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/password:<*password*>	Specify the password for the username specified in the **/username** parameter.
/anonpass1:<*password*>	(Optional) If the source database is anonymized, key in the primary anonymization password to decrypt import data.
/anonpass2:<*password*>	(Optional) If the source database is anonymized, using two anonymization keys, key in the secondary anonymization password to decrypt import data.

Example

```
EsmDlibM.exe /importFromSQL /server:192.168.11.11
/database:EventsDatabase /dbauth:SQL /username:sa /password:p@ss
/anonpass1:p@ss
```

16.2.2 /importFromDlib

This function enables you to import data that was exported from a database server (DLIB) of an older version of GFI EventsManager. The following parameters are supported:

Table 106: /importFromDlib Parameters

Parameter	Description
/path:<*path*>	Specify the path to the DLib database server. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/name:<*name*>	Specify the name of the DLib database you want to import. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/anonpass1:<*password*>	(Optional) If the source database is anonymized, key in the primary anonymization password to decrypt import data.

Parameter	Description
/anonpass2:<*password*>	(Optional) If the source database is anonymized, using two anonymization keys, key in the secondary anonymization password to decrypt import data.

Example

```
EsmDlibM.exe /importFromDlib /path:C:\DLibServer /name:EventsData
/anonpass1:p@ss
```

16.2.3 /copyData

This function enables you to copy data from one DLib database server to another. The following parameters are supported:

Table 107: /copyData Parameters

Parameter	Description
/destinationPath:<*destinationPath*>	Specify the destination database server. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/destinationName:<*destinationName*>	Specify the destination database name. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/destinationEncPass:<*password*>	(Optional) Specify a password to encrypt data at the destination.
/sourcePath:<*sourcePath*>	Specify the path to the source database server. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/sourceName:<*sourceName*>	Specify the name of the source database. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/sourceEncPass:<*password*>	(Optional) Specify an encryption key to encrypt source data.
/anonpass1:<*password*>	(Optional) Specify the primary anonymization password to anonymize source data.
/anonpass2:<*password*>	(Optional) Specify a secondary anonymization password to anonymize source data using two keys.

Parameter	Description
/period:<*type*><*number*><*unit*>	Enables you to filter by event date to get events from the last days/weeks/months or older than days/weeks/months. For instance, to filter events that happened in the Last 24 Days, the parameter value is: **l24d**. And to filter events Older than 3 Weeks, the parameter value is **O3W**. Supported values include: » <type>: • **o** - older than • **l** - last » <number> - specify the number of days/weeks/months » <unit>: • **d** - days • **w** - weeks • **m** - months.
/markEventsAsDeleted	(Optional) Mark copied events as deleted from the source database. These events will no longer be visible in the management console but will still remain in the database. To completely remove them from the database, run **Commit Deletions** job.
/log_format:***<value>*** /machine:***<value>*** /importance:<value> /occured:***<value>***	These parameters provide the user a convenient way to filter events by the corresponding columns. Any of these filters are optional. When used together, they are linked in an AND condition on the source data. Except for machine, where the user may enter the targeted machine name as displayed in events browser, the other parameters have predefined values with obvious meaning, that are listed below. Supported values are: » log_format: • "windows • sql audit • oracle audit • text logs • syslog messages • snmp traps • monitoring » importance • Unclassified • Low • Medium • High • Critical • Noise » occurred • Today • Yesterday • Last 7 days • Last 30 days • This month • Last month.

Example

```
EsmDlibM.exe /copyData /destinationPath:Z:\DestServ
/destinationName:DestData /sourcePath:C:\SourServ
/sourceName:SourData /sourceEncPass:p@ss /markEventsAsDeleted
```

16.2.4 /importFromLegacyFile

This function enables you to import data that was exported to files from an older version of GFI EventsManager. The following parameters are supported:

Table 108: /importFromLegacyFile Parameters

Parameter	Description
/path:<*path*>	Specify the path to the import file. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/logTypes:<*application*, *custom*, *directory*, *security*, *dns*, *filereplication*, *syslog*, *system*, *snmp*, *oracle*, *sql*, *text*>	(Optional) Specify the log types you want to import. Exclude parameter to import all log types.
/password:<*password*>	(Optional) Specify a password to decrypt import data.
/anonpass1:<*password*>	(Optional) Specify the primary anonymization password to anonymize import data.
/anonpass2:<*password*>	(Optional) Specify a secondary anonymization password to anonymize import data using two keys.

Example

```
EsmDlibM.exe /importFromLegacyFile
/path:C:\ImportData\Configuration.cfg /password:p@ss /anonpass1:p@ss
```

16.2.5 /exportToFile

This function enables you to export data from a DLib database server to another one as part of the data centralization process. You can also use this function to backup your data for safekeeping. The following parameters are supported:

Table 109: /exportToFile

Parameter	Description
/path:<*path*>	Specify the folder path where data is exported to. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/sourceEncPass:<*password*>	(Optional) Specify a password to encrypt source data.
/destinationEncPass:<*password*>	(Optional) Specify a password to encrypt destination data.
/anonpass1:<*password*>	(Optional) If the source database is anonymized, key in the primary anonymization password to decrypt exported data.
/anonpass2:<*password*>	(Optional) If the source database is anonymized using two anonymization keys, key in the secondary anonymization password to decrypt export data.

Parameter	Description
/period:<*type*><*number*><*unit*>	Enables you to filter by event date to get events from the last days/weeks/months or older than days/weeks/months. For instance, to filter events that happened in the Last 24 Days, the parameter value is: **l24d**. And to filter events Older than 3 Weeks, the parameter value is **O3W**. Supported values include: » <type>: • **o** - older than • **l** - last » <number> - specify the number of days/weeks/months » <unit>: • **d** - days • **w** - weeks • **m** - months.
/markEventsAsDeleted	(Optional) Mark copied events as deleted from the source database. These events will no longer be visible in the management console but will still remain in the database. To completely remove them from the database, run **Commit Deletions** job.
/log_format:***<value>*** /machine:***<value>*** /importance:<value> /occured:***<value>***	These parameters provide the user a convenient way to filter events by the corresponding columns. Any of these filters are optional. When used together, they are linked in an AND condition on the source data. Except for machine, where the user may enter the targeted machine name as displayed in events browser, the other parameters have predefined values with obvious meaning, that are listed below. Supported values are: » log_format: • "windows • sql audit • oracle audit • text logs • syslog messages • snmp traps • monitoring » importance • Unclassified • Low • Medium • High • Critical • Noise » occurred • Today • Yesterday • Last 7 days • Last 30 days • This month • Last month.

Example

```
EsmDlibM.exe /exportToFile /path:C:\ExportedDataFolder
/sourceEncPass:p@ss /markEventsAsDeleted /importance:High
```

16.2.6 /importFromFile

This function enables you to import data from a file as part of the data centralization process. The import file must be created from an **Export to File** job. The following parameters are supported:

Table 110: /importFromFile Parameters

Parameter	Description
/path:<*path*>	Specify the path to where the import file is saved. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/password:<*password*>	(Optional) If the import file is password protected, key in the password.
/log_format:<***value***> /machine:<***value***> /importance:<value> /occured:<***value***>	These parameters provide the user a convenient way to filter events by the corresponding columns. Any of these filters are optional. When used together, they are linked in an AND condition on the source data. Except for machine, where the user may enter the targeted machine name as displayed in events browser, the other parameters have predefined values with obvious meaning, that are listed below. Supported values are: » log_format: • "windows • sql audit • oracle audit • text logs • syslog messages • snmp traps • monitoring » importance • Unclassified • Low • Medium • High • Critical • Noise » occurred • Today • Yesterday • Last 7 days • Last 30 days • This month • Last month.

Example

```
EsmDlibM.exe /importFromFile /path:C:\ImportFolder\Import.cfg
/password:p@ss /machine:MS11.domain.com /occured:true
```

16.2.7 /commitDeletedRecords

This function enables you to delete events that are marked as deleted from the database. The following parameters are supported:

Table 111: /commitDeletedRecords Parameters

Parameter	Description
/dbPath:<*dbPath*>	Specify the path to the database server which contains events marked as deleted. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/password:<*password*>	(Optional) If the database is password protected, key in the password.
/anonpass1:<*password*>	(Optional) If the database is anonymized, key in the password to remove anonymization.
/anonpass2:<*password*>	(Optional) If the database is anonymized using two anonymization keys, key in the secondary key.

Example

```
EsmDlibM.exe /commitDeletedRecords /dbpath:C:\DatabaseServerFolder
/password:p@ss /anonpass1:pa$$
```

16.2.8 /exoportToSQL

This function enables you to export specified event to SQL Server®. The following parameters are supported:

Table 112: /exportToSQL Parameters

Parameter	Description
/server:<*serverName*>	Specify the IP address or computer name running SQL Server®. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/database:<*maindb*|*backupdb*>	Specify the name of the destination database. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/dbauth:<*SQL*|*WIN*>	Specify the authentication mode configured in the source SQL Server®. Supported values include: » **SQL**: to use SQL Server® authentication » **WIN**: to use Windows® authentication.
/username:<*username*	Specify a username that has access to the database from which you want to import data. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/password:<*password*>	Specify the password for the username specified in the **/username** parameter.

Parameter	Description
/table:<*table*>	Specify the name of the destination table. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/period:<*type*><*number*><*unit*>	Enables you to filter by event date to get events from the last days/weeks/months or older than days/weeks/months. For instance, to filter events that happened in the Last 24 Days, the parameter value is: **l24d**. And to filter events Older than 3 Weeks, the parameter value is **O3W**. Supported values include: » <type>: • **o** - older than • **l** - last » <number> - specify the number of days/weeks/months » <unit>: • **d** - days • **w** - weeks • **m** - months.
/sourceEncPass:<*password*>	(Optional) If the source data is encrypted, key in the password to decrypt exported data.
/anonpass1:<*password*	(Optional) If the source database is anonymized, key in the primary anonymization password to decrypt exported data.
/anonpass2:<*password*>	(Optional) If the source database is anonymized using two anonymization keys, key in the secondary anonymization password to decrypt export data.

Example

```
EsmDlibM.exe /exportToSQL /server:192.168.11.11
/database:EventsDatabase /dbauth:SQL /username:sa /password:p@ss
/table:EventsTable /anonpass1:pa$$
```

16.3 Using DLibAdm.exe

DLibAdm.exe is used to run administrative operations on DLib Database Servers installed on the network.

To use DLibAdm.exe:

1. Click **Start > Run** and key in **CMD**.

2. Click **Ctrl + Shift + Enter** to run **CMD** as an administrator.

3. Change the active directory to the install folder of DLib Database Server. Key in (example):

```
CD C:\Program Files\GFI\Database Server 2.0
```

Press **Enter**.

4. Key in **DLibAdm.exe** followed by the functions described below:

» /decryptDatabase

» /encryptDatabase

» /displayAllDLib

» /copyMoveDLib

16.3.1 /decryptDatabase

This function enables you to decrypt an encrypted DLib database. The following parameters are supported:

Table 113: /decryptDatabase Parameters

Parameter	Description
/dbPath:<*path*>	Specify the path to the database you want to decrypt. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/dbName:<*name*>	Specify the name of the database you want to decrypt. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/password:<*password*>	Specify the password used to decrypt the database.

Example

```
DLibAdm.exe /decryptDatabase /dbPath:"C:\Program Files\GFI\Database
Server 2.0" /dbName:EventsDatabase /password:p@ss
```

16.3.2 /encryptDatabase

This function enables you to encrypt a specified database. The following parameters are supported:

Table 114: /encryptDatabase Parameters

Parameter	Description
/dbPath:<*path*>	Specify the path to the database you want to encrypt. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/dbName:<*name*>	Specify the name of the database you want to encrypt. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/password:<*password*>	Specify the password used to encrypt the database.

Example

```
DLibAdm.exe /encryptDatabase /dbPath:"C:\Program Files\GFI\Database
Server 2.0" /dbName:EventsDatabase /password:p@ss
```

16.3.3 /displayAllDLib

This function enables you to list all the valid DLib Database Servers running in a specified folder. The following parameter is supported:

Table 115: /displayAllDLib Parameters

Parameter	Description
/path:<*path*>	Specify the folder path where you want to scan for valid DLib Database Servers. **Note** Parameters that contain spaces must be enclosed in double quotes (“).

Example

```
DLibAdm.exe /displayAllDLib /path:"C:\Program Files\GFI\Database
Server 2.0"
```

16.3.4 /copyMoveDLib

This function enables you to copy or move a DLib database to a specified location. The following parameters are supported:

Table 116: /copyMoveDLib

Parameter	Description
/sourcePath:<*sourcePath*>	Specify the path to the source database (database you want to move or copy). **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/destinationPath:<*destinationPath*>	Specify the path to the destination folder. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/copyMove:<*copy*|*move*>	Specify the action to perform on the database. Supported values: » copy » move.
/dbName:<*dbName*>	Specify the name of the database you want to copy or move. **Note** Parameters that contain spaces must be enclosed in double quotes (“).

Exmaple

```
DLibAdm.exe /copyMoveDLib /sourcePath:"C:\Program Files\GFI\Database
Server 2.0" /destinationPath:C:\EventsDatabases /copyMove:move
/dbName:EventsDatabase
```

16.4 Using EsmReport.exe

EsmReport.exe enables you to generate in-product reports such as configuration and job activity reports.

To use EsmReport.exe:

1. Click **Start > Run** and key in **CMD**.

2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.

3. Change the directory to the GFI EventsManager install directory. Example:

```
CD <C:\Program Files\GFI\EventsManager>
```

4. Key in **EsmReport.exe** followed by any of the following functions:

- Generate Configuration reports
- Generate Status reports
- Generate Events reports

16.4.1 Generate Configuration reports

This function enables you to generate Configuration reports about a single or group of event sources. The following parameters are supported:

Table 117: Configurations report parameters

Parameter	Description
/type:<*configuration*|*status*|*events*>	Specify the type of report you want to generate. Supported values are: » configuration » status » events. Key in **/type:configuration** to generate a configuration report.
/target:<*path*>	Specify the folder path where the generated report is saved. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/format:<*html*|*csv*>	Specify the format of the report. Supported values are: » html » csv.
/source:<*name*>	Specify the event source name. Use this parameter to generate a configuration report about a single event source. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/group:<*name*>	Specify the event source group name. Use this parameter to generate a configuration report about a group of event sources. **Note** Parameters that contain spaces must be enclosed in double quotes (“).

Example

```
EsmReport.exe /type:configuration /target:C:\ReportsFolder
/format:html /group:"Domain Controllers"
```

16.4.2 Generate Status reports

This function enables you to generate GFI EventsManager Status reports. The following parameters are supported:

Table 118: Status report parameters

Parameter	Description
/type:<*configuration*|*status*|*events*>	Specify the type of report you want to generate. Supported values are: » configuration » status » events. Key in **/type:status** to generate a status report.
/subtype:<*messages*|*stats*>	Specify the type of status report you want to generate. Supported values are: » **messages** - when messages is specified, the following parameters can be used: • **/period:<*current*|*date*>** - key in **current** to generate a report containing messages generated on the same day. Else key in a date to generate a status report containing messages generated on the specified date. » **stats** - when stats is specified as a subtype, the following parameters can be used: • **/format:<*html*|*csv*>** - specify the format of the report. Supported values are **HTML** and **CSV** • **/period:<*"all time"*|*date*>** - specify the timeframe that the report is based on. Supported values include **"all time"** or else a specific date • **/options:<*"error messages"*|*"only with issues"*>** - specify the type of stats to generate. Supported values are **"error messages"** and **"only with issues"** • **/target:<*path*>** - specify the folder path where the report is saved. **Note** Parameters that contain spaces must be enclosed in double quotes (“).

Messages example

```
EsmReport.exe /type:status /subtype:messages /period:"current date"
```

Stats example

```
EsmReport.exe /type:status /subtype:stats /format:html
/period:20130111 /options:"error messages" /target:C:\StatsReports
```

16.4.3 Generate Events reports

This function enables you to generate Events reports. The following parameters are supported:

Table 119: Events reports parameters

Parameter	Description
/type:<*configuration*|*status*|*events*>	Specify the type of report you want to generate. Supported values are: » configuration » status » events. Key in **/type:events** to generate an events report.

Parameter	Description
/repname:<*fullReportName*>	Specify a name for the generated report. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/repid:<*reportID*>	Specify a unique ID for the generated report. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/target<*path*>	Specify the folder path where the report is saved. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/format:<*html*|*csv*>	Specify the format of the report. Supported values are: » html » csv.
/datefrom:<*startDate*>	Specify the start date of the timeframe to report on.
/dateto:<*endDate*>	Specify the end date of the timeframe to report on.
/scheduled	Specify this parameter to generate the report based on schedule settings configured in the Management Console.

Example

```
EsmReport.exe /type:events /repname:"New Events Report" /repid:11
/target:C:\ReportsFolder /format:html /datefrom:20121201
/dateto:20130111
```

16.4.4 Using ImportSettings.exe

Importsettings.exe enables you to import configuration from a data folder or from a configuration file that was exported from another instance of GFI EventsManager. Use this tool to backup configuration settings of the Management Console.

To use ImportSettings.exe:

1. Click **Start > Run** and key in **CMD**.
2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.
3. Change the directory to the GFI EventsManager install directory. Example:

```
CD <C:\Program Files\GFI\EventsManager>
```

4. Key in **ImportSettings.exe** followed by the parameters described below:

Table 120: CMD: ImportSettings.exe parameters

Parameter	Description
/operation: <*operation*>	Specify the operation to perform. Supported values are: » importFile » importFolder.
/destination: <*folder*>	Specify the destination folder where configuration is imported. **Note** Parameters that contain spaces must be enclosed in double quotes (“).

Parameter	Description
/sourceFile:<*file-name*>	Specify the file name that contains exported configurations. Use this parameter to define the file name when running an **importFile** operation. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/sourceFolder: <*folder name*>	Specify the folder name that contains exported configurations. Use this parameter to define the folder name when running an **importFolder** operation. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/id:<*EsmInstanceID*>	This parameter can only be used when you want to change the instance ID of GFI EventsManager. If no value is specified, the same ID is preserved. If you do not use this parameter, **/operation**, **/destination**, **/sourceFile** or **/sourceFolder** parameters are mandatory.

Example

```
ImportSettings.exe /operation:importFile
/destination:C:\NewDestination /sourceFile:C:\ExportedSettings
```

OR

```
ImportSettings.exe /id:newInstanceID
```

16.4.5 Using ExportSettings.exe

ExportSettings.exe enables you to export configuration settings from GFI EventsManager to a configuration file.

To use ExportSettings.exe:

1. Click **Start > Run** and key in **CMD**.
2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.
3. Change the directory to the GFI EventsManager install directory. Example:

```
CD <C:\Program Files\GFI\EventsManager>
```

4. Key in **ExportSettings.exe** followed by the parameters described below:

Table 121: CMD: ExportSettings.exe parameters

Parameter	Description
/destination: <*fileName*>	Specify a valid folder path including file name where settings are exported to. Unless specified, **.esmbkp** is appended as an extension to the file name. **Note** Parameters that contain spaces must be enclosed in double quotes (“).
/folder: <*folder*>	This parameter is used to instruct the tool to export settings from another location than the default Data folder. Specify the folder path containing GFI EventsManager data settings to be exported. **Note** Parameters that contain spaces must be enclosed in double quotes (“).

Example

```
ExportSettings.exe /destination:C:\NewDestination
```

17 Miscellaneous

This chapter provides you with information related to configuring Third-Party components required for GFI EventsManager auditing operations. Learn how to configure and run GFI EventsManager actions through the provided command line tools.

Topics in this chapter:

17.1 Enabling event source permissions manually 326

17.2 Enabling event source permissions automatically 334

17.3 Disabling User Account Control (UAC) 339

17.1 Enabling event source permissions manually

This section describes how to configure permissions that are required by GFI EventsManager to audit systems and process the necessary events. This process has to be done on each machine to scan.

This section contains information about:

- Enabling permissions on Microsoft® Windows® XP
- Enabling permissions on Microsoft® Windows® Vista
- Enabling permissions on Microsoft® Windows® 7
- Enabling permissions on Microsoft® Windows® Server 2003
- Enabling permissions on Microsoft® Windows® Server 2008 (including R2)

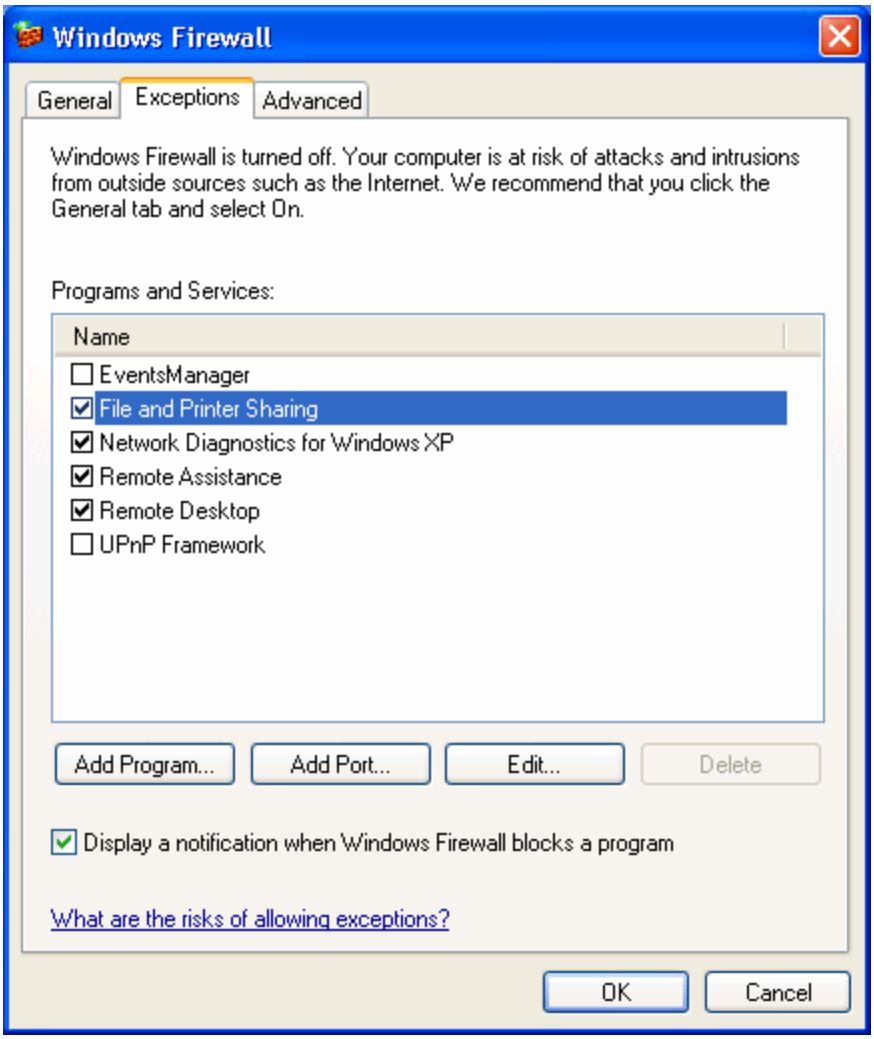
Note

In an active directory environment, permissions can be set automatically via Group Policy Object (GPO). For more information refer to Enabling event source permissions automatically.

17.1.1 Enabling permissions on Microsoft® Windows® XP

To enable permissions Microsoft® Windows® event sources:

1. Click **Start > Control Panel > Windows Firewall > Exceptions** tab.



Screenshot 277: Firewall rules on Microsoft® Windows® XP

2. From **Programs and Services** list, enable **File and Printer Sharing**.

3. Click **OK**.

17.1.2 Enabling permissions on Microsoft® Windows® Vista

To enable permissions on machines running Microsoft® Windows® Vista:

- Step 1: Enable Firewall permissions
- Step 2: Enable additional auditing features

Step 1: Enable Firewall permissions

1. Click **Start > Control Panel > Security** and click **Allow a program through Windows Firewall** from the left panel.

2. Select **Exceptions** tab and from **Allowed programs and features** list, enable the following rules:

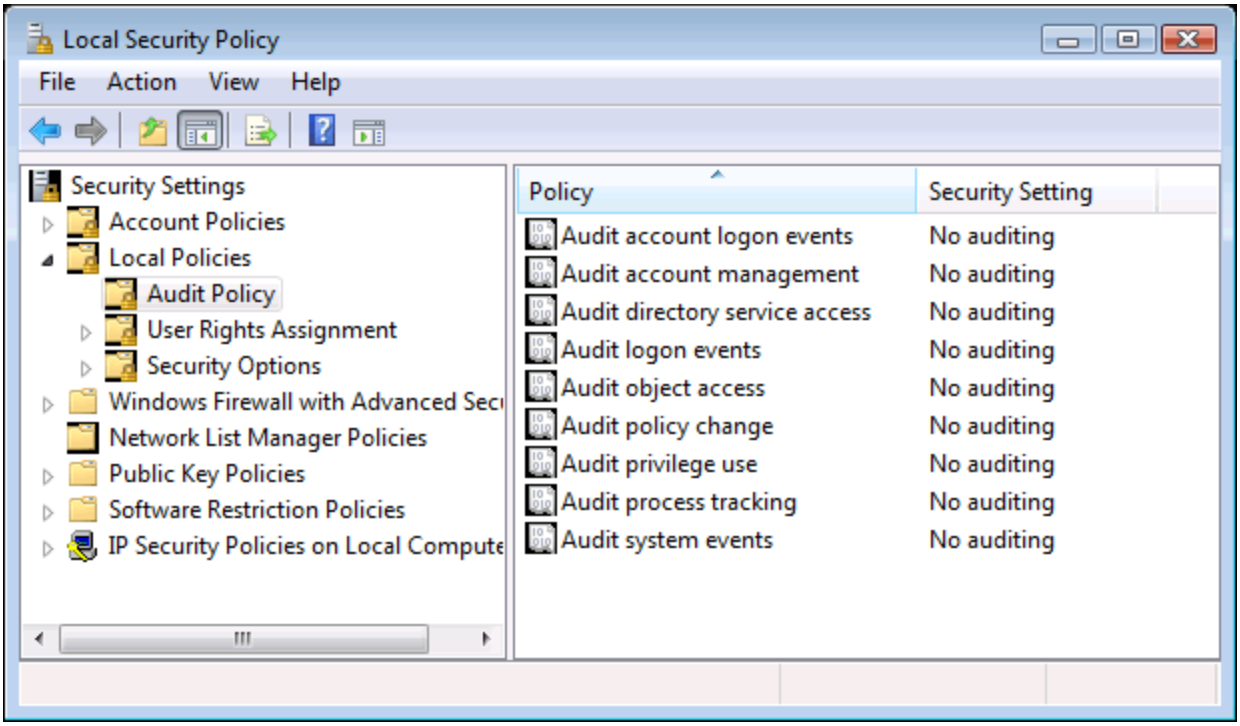
- Remote Event Log Management
- File and Printer Sharing
- Network Discovery.

3. Click **Apply**.

Step 2: Enable additional auditing features

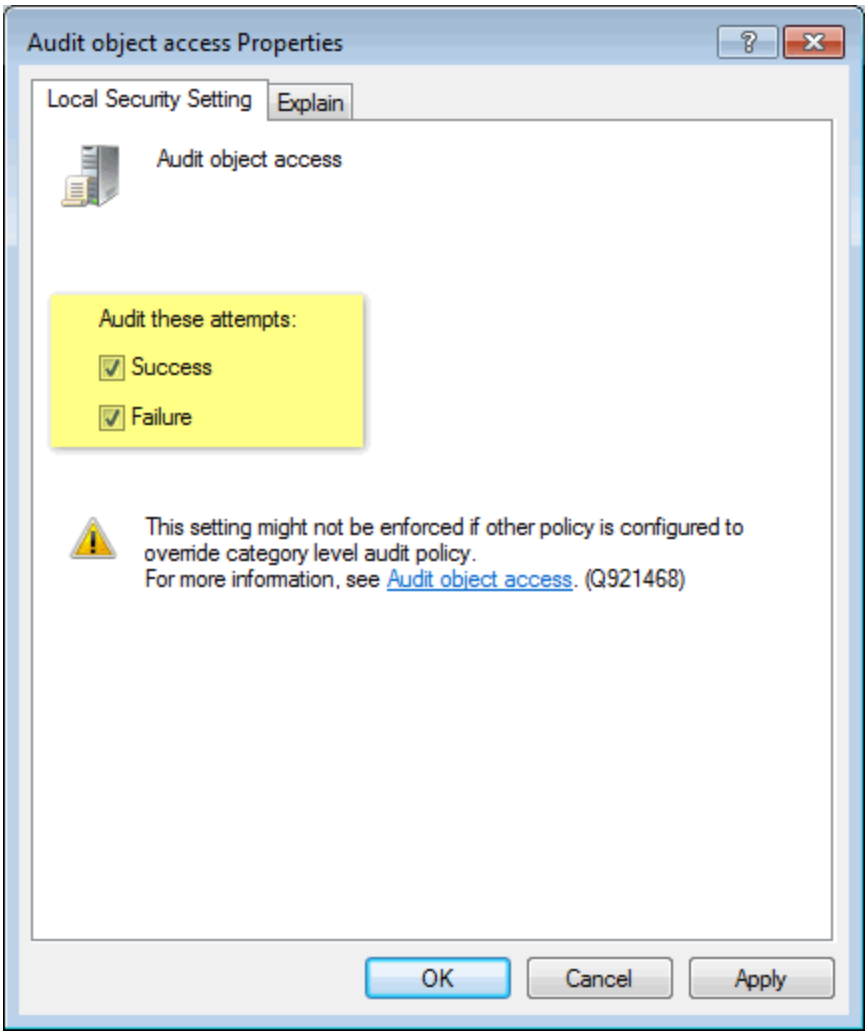
1. Click **Start > Run** and key in **secpol.msc**. Press **Enter**.

2. From the **Security Settings** node, expand **Local Policies > Audit Policy**.



Screenshot 278: Local security policy window

3. From the right panel, double-click **Audit object access**.



Screenshot 279: Audit object access properties

4. From the **Audit object access Properties**, select **Success** and **Failure** and click **OK**.
5. From the right panel, double-click **Audit Process tracking**.
6. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.
7. From the right panel, double-click **Audit account management**.
8. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.
9. From the right panel, double-click **Audit system events**.
10. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.
11. Close the Local Security Policy window.

17.1.3 Enabling permissions on Microsoft® Windows® 7

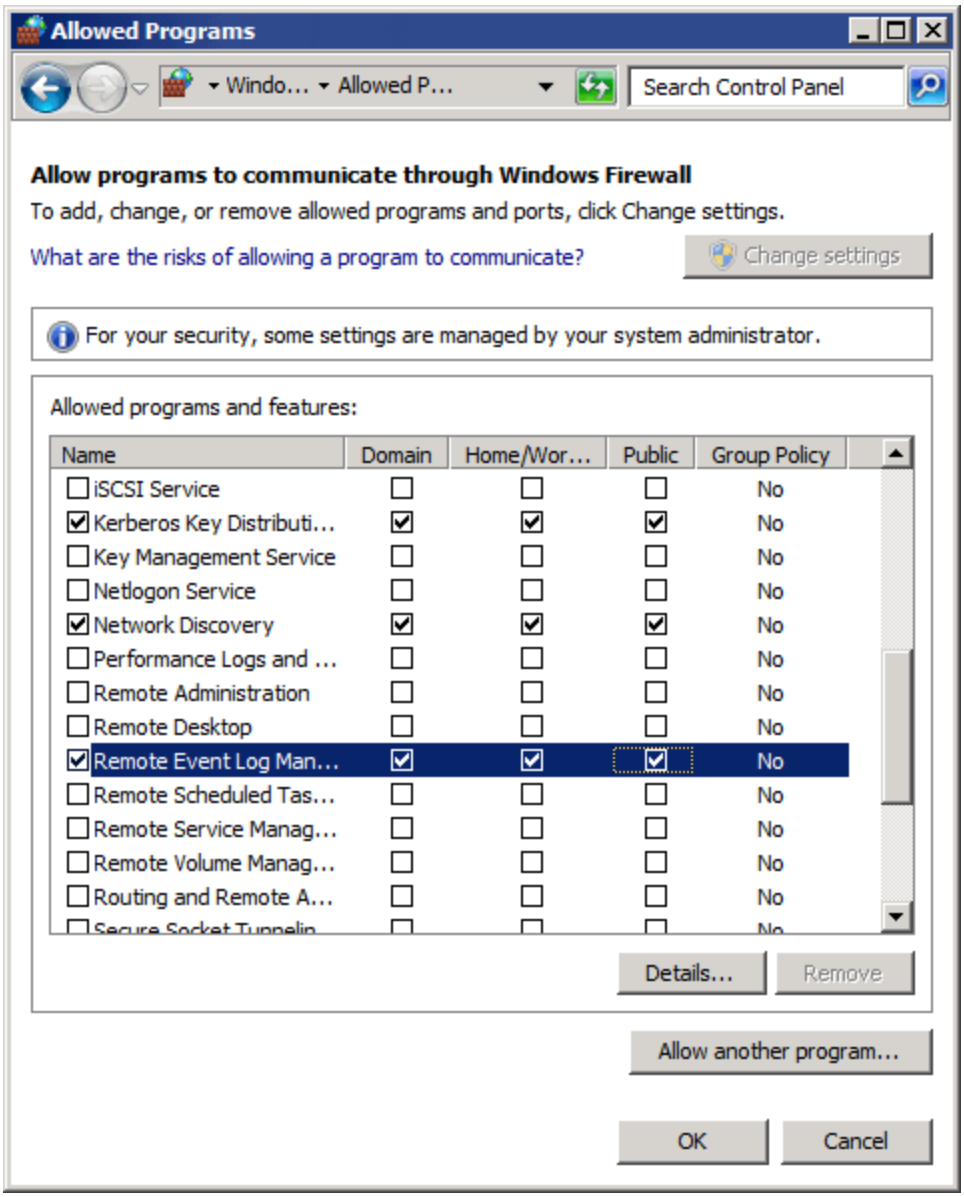
To enable permissions on machines running Microsoft® Windows® 7:

- Step 1: Enable Firewall permissions
- Step 2: Enable additional auditing features

Step 1: Enable Firewall permissions

To manually enable firewall rules on Microsoft® Windows® 7:

1. Click **Start > Control Panel > System and Security** and click **Allow a program through Windows Firewall**, under Windows Firewall category.



Screenshot 280: Allowed programs in Microsoft® Windows® Vista or later

2. From **Allowed programs and features** list, enable the following rules:

- Remote Event Log Management
- File and Printer Sharing
- Network Discovery.

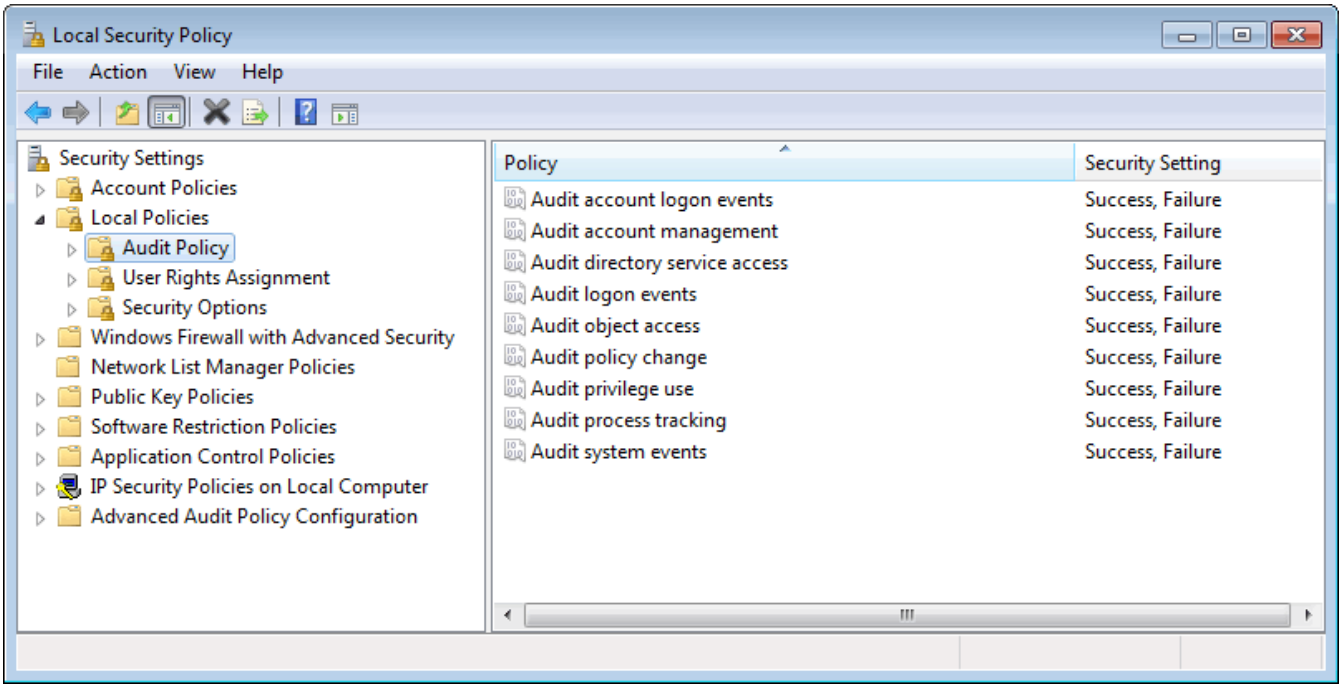
3. Select **Domain**, **Private** and **Public** for each rule mentioned above.

4. Click **OK**.

Step 2: Enable additional auditing features

1. Click **Start** > **Run** and key in **secpol.msc**. Press **Enter**.

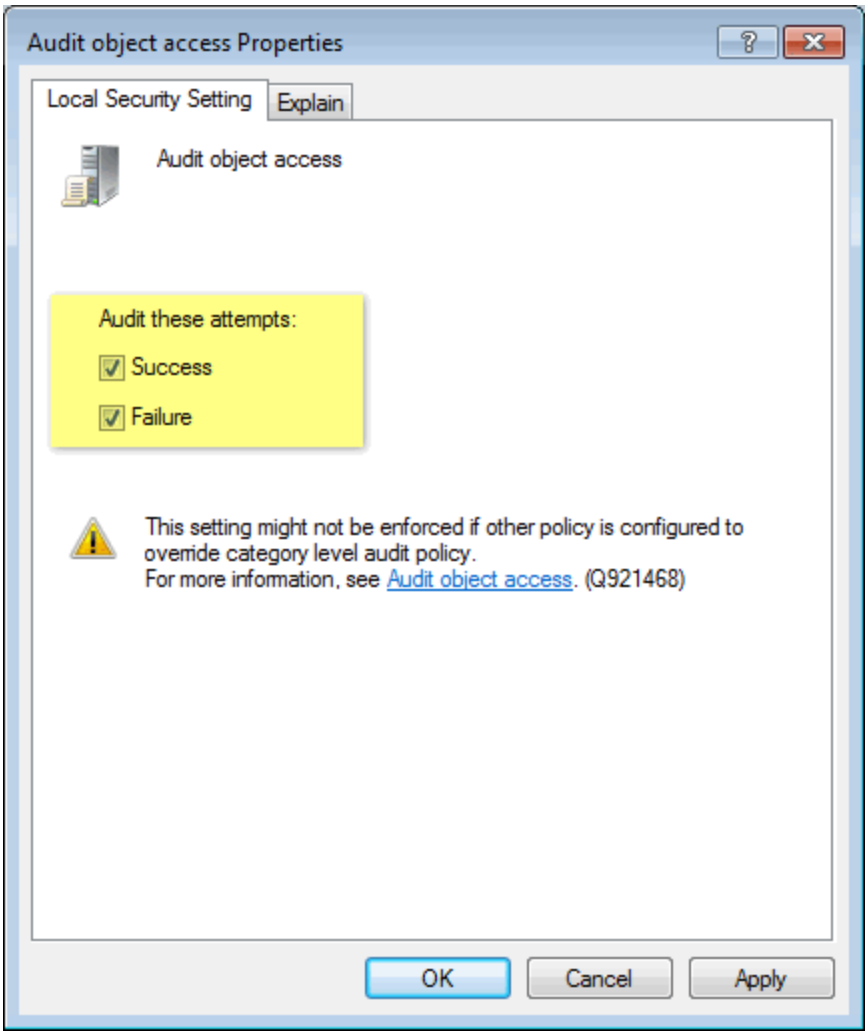
2. From the **Security Settings** node, expand **Local Policies** > **Audit Policy**.



Screenshot 281: Local security policy window

3. From the right panel, double-click **Audit object access**.

4. From **Audit object access Properties**, select **Success** and **Failure**. Click **OK**.



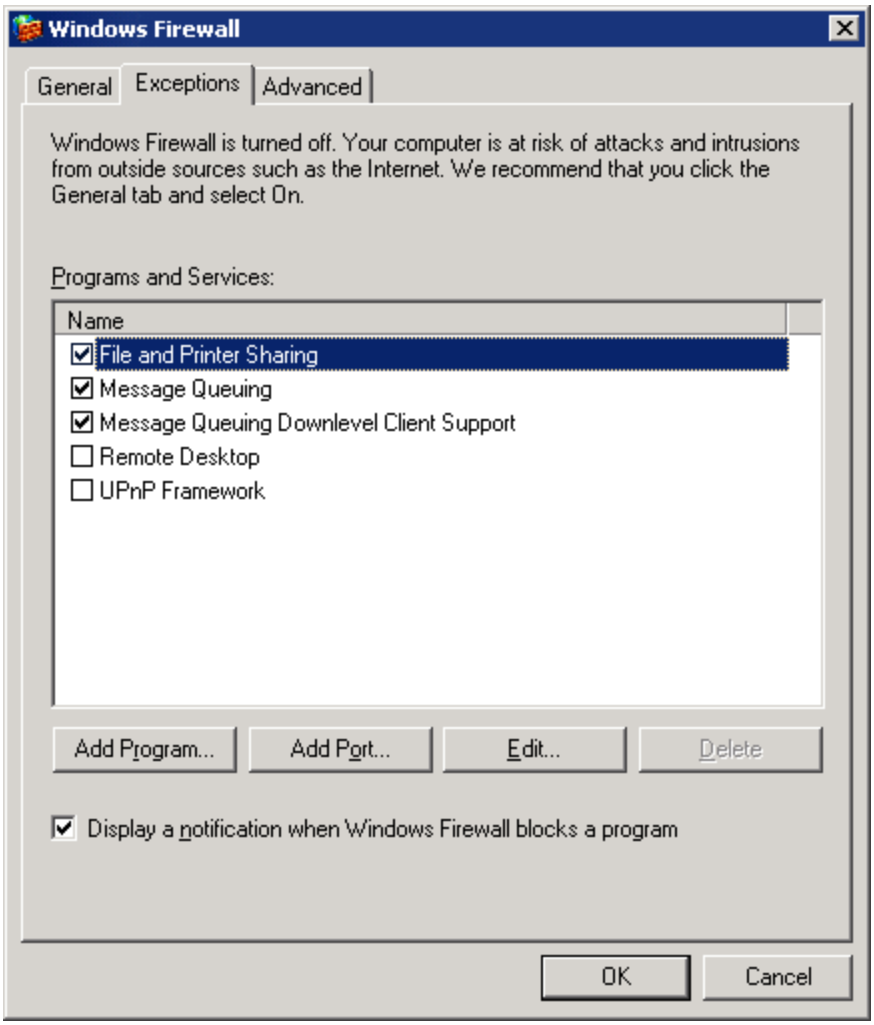
Screenshot 282: Audit object access Properties

5. From the right pane, double-click **Audit Process tracking**.
6. From **Audit process tracking Properties**, select **Success** and **Failure**. Click **OK**.
7. From **Audit process tracking Properties**, select **Success** and **Failure**. Click **OK**.
8. From the right panel, double-click **Audit account management**.
9. From **Audit process tracking Properties**, select **Success** and **Failure**. Click **OK**.
10. From the right panel, double-click **Audit system events**.
11. From **Audit process tracking Properties**, select **Success** and **Failure**. Click **OK**.
12. Close the local Security Policy window.

17.1.4 Enabling permissions on Microsoft® Windows® Server 2003

To manually enable firewall rules on Microsoft® Windows® Server 2003:

1. Click **Start > Control Panel > Windows Firewall** and select **Exceptions** tab.



Screenshot 283: Enable firewall rules in Microsoft® Windows® Server 2003

2. From **Programs and Services** list, enable **File and Printer Sharing**.

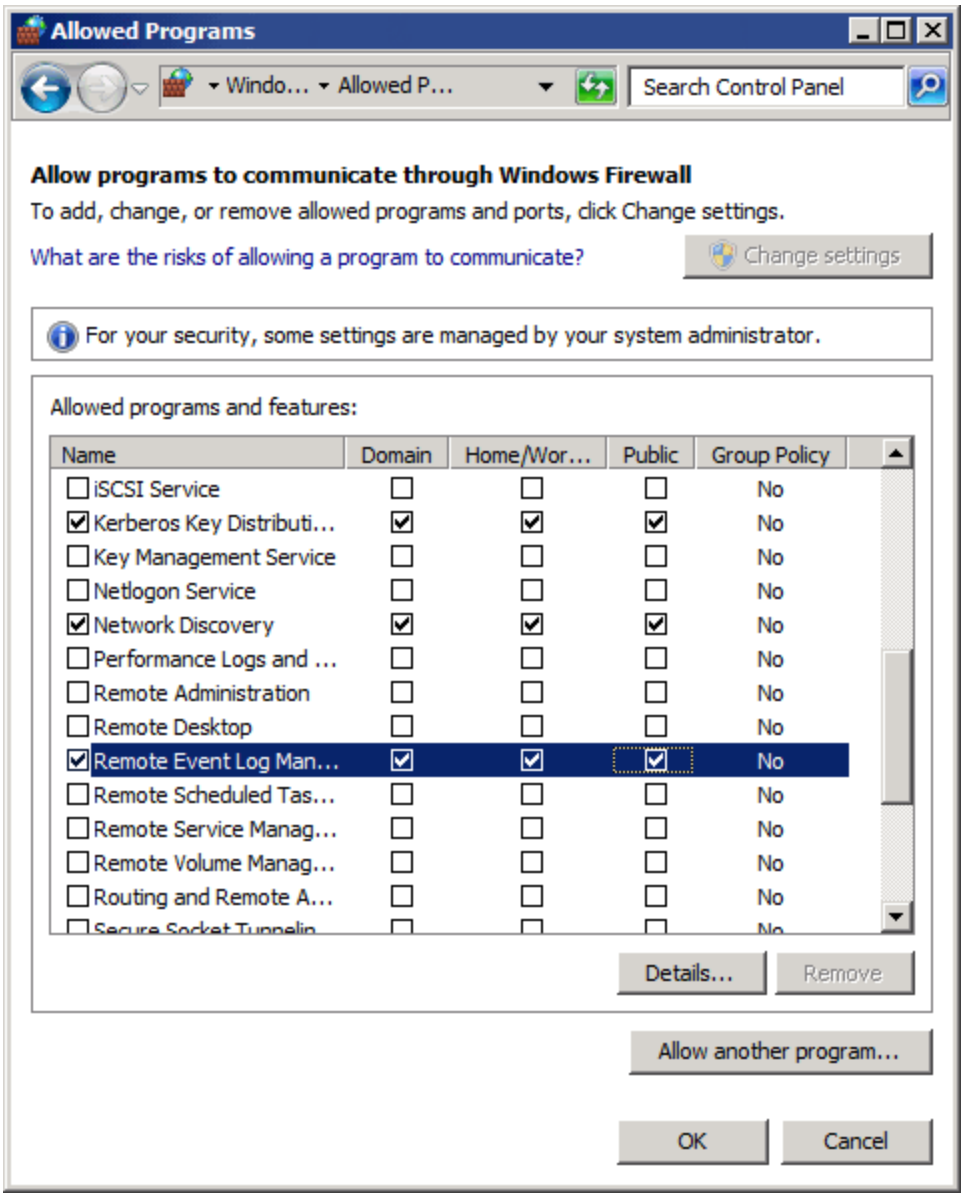
3. Click **OK**.

17.1.5 Enabling permissions on Microsoft® Windows® Server 2008 (including R2)

1. Click **Start > Control Panel > Security** and click **Allow a program through Windows Firewall** under **Windows Firewall** category.

2. In the list of programs, enable the following:

- File and Printer Sharing
- Network Discovery
- Remote Event Log Management.



Screenshot 284: Firewall rules on Microsoft® Windows® Server 2008

3. Click **OK**.

> **Note**
>
> In Windows® Server 2008 R2, ensure to select **Domain**, **Private** and **Public** for each rule mentioned above.

17.2 Enabling event source permissions automatically

This section contains information about:

- Enabling permissions on Windows® Server 2003 via GPO
- Enabling permissions on Windows® Server 2008 via GPO

17.2.1 Enabling permissions on Windows® Server 2003 via GPO

To open enable permissions on all domain clients using Microsoft® Windows® Server 2003 domain controller:

1. Click **Start > Run**, key in **mmc**. Press **Enter**.

2. Click **File > Add/Remove Snap-in** and click **Add**.

3. Locate and select **Group Policy Object Editor** and click **Add**.

4. Click **Browse**, select **Default Domain Policy** and click **OK**.

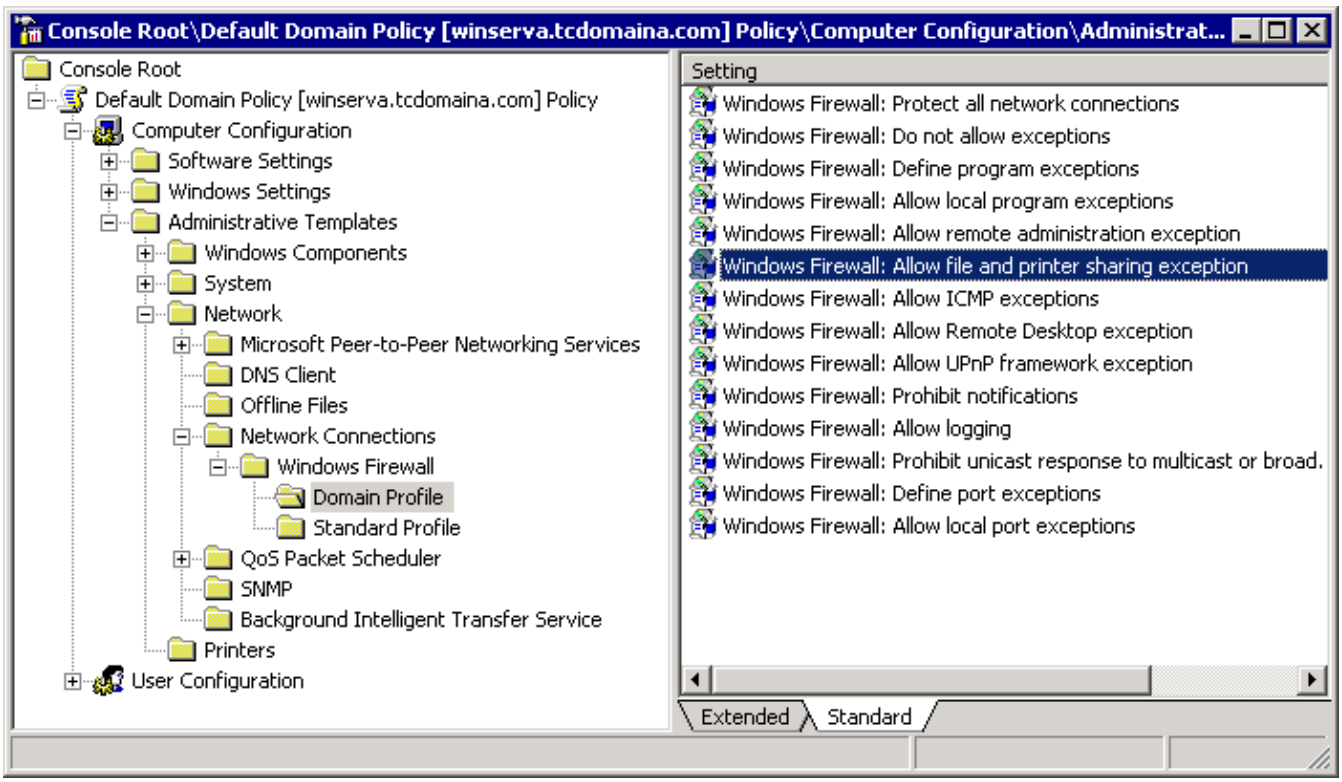
5. Click **Finish**.

6. Select **Group Policy Object Editor** again and click **Add**.

7. Click **Browse**, double-click **Domain Controllers** folder and select **Default Domain Controllers Policy**. Click **OK**.

8. Click **Finish** and **Close**.

9. From **Console Root**, expand **Default Domain Policy > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile**.



Screenshot 285: Domain Policy console in Microsoft® Windows® Server 2003

10. From **Setting** list, right-click **Windows Firewall: Allow file and printer sharing exception** and select **Properties**.

11. From the **Settings** tab, select **Enabled** and click **OK**.

12. Repeat steps 9 to 11 for **Default Domain Controllers Policy**.

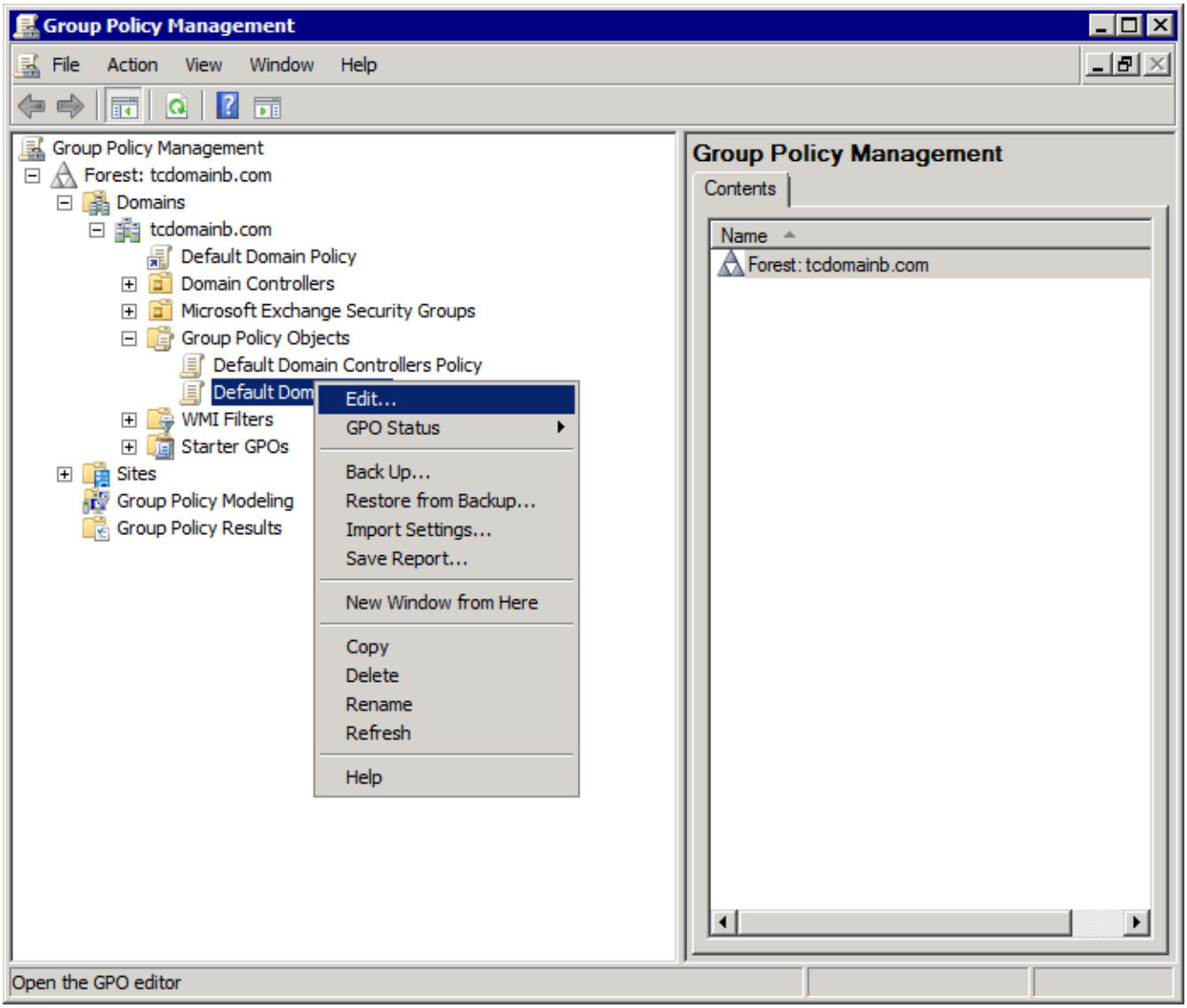
13. Click **File > Save** to save the management console. The group policy comes into effect the next time each machine is restarted.

17.2.2 Enabling permissions on Windows® Server 2008 via GPO

To enable permissions on all domain clients:

1. Click **Start > Administrative Tools > Group Policy Management**.

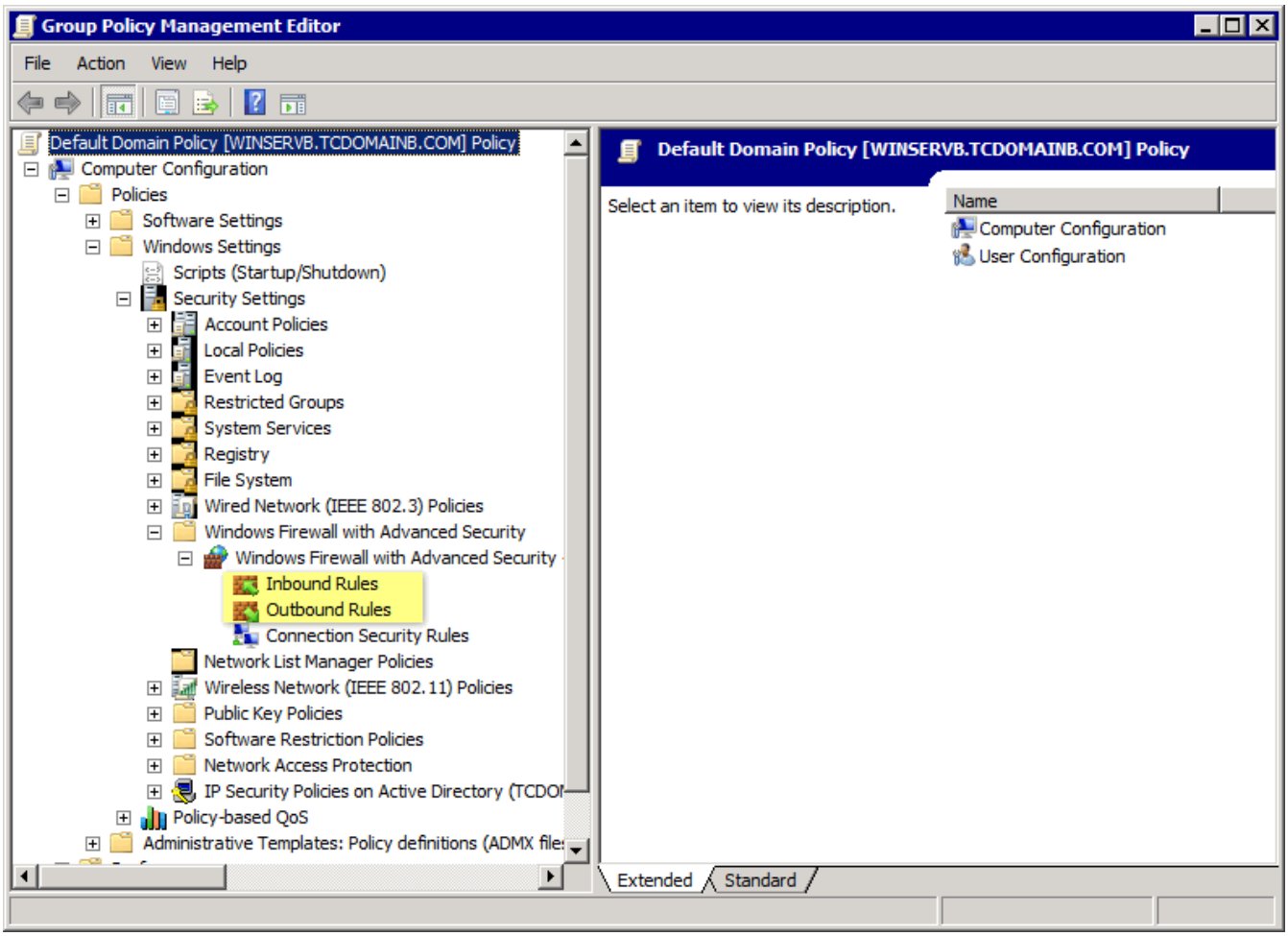
2. Expand **Group Policy Management > Forest > Domains > <*Domain name*> > Group Policy Objects**.



Screenshot 286: Group Policy Management in Microsoft® Windows® Server 2008 R2

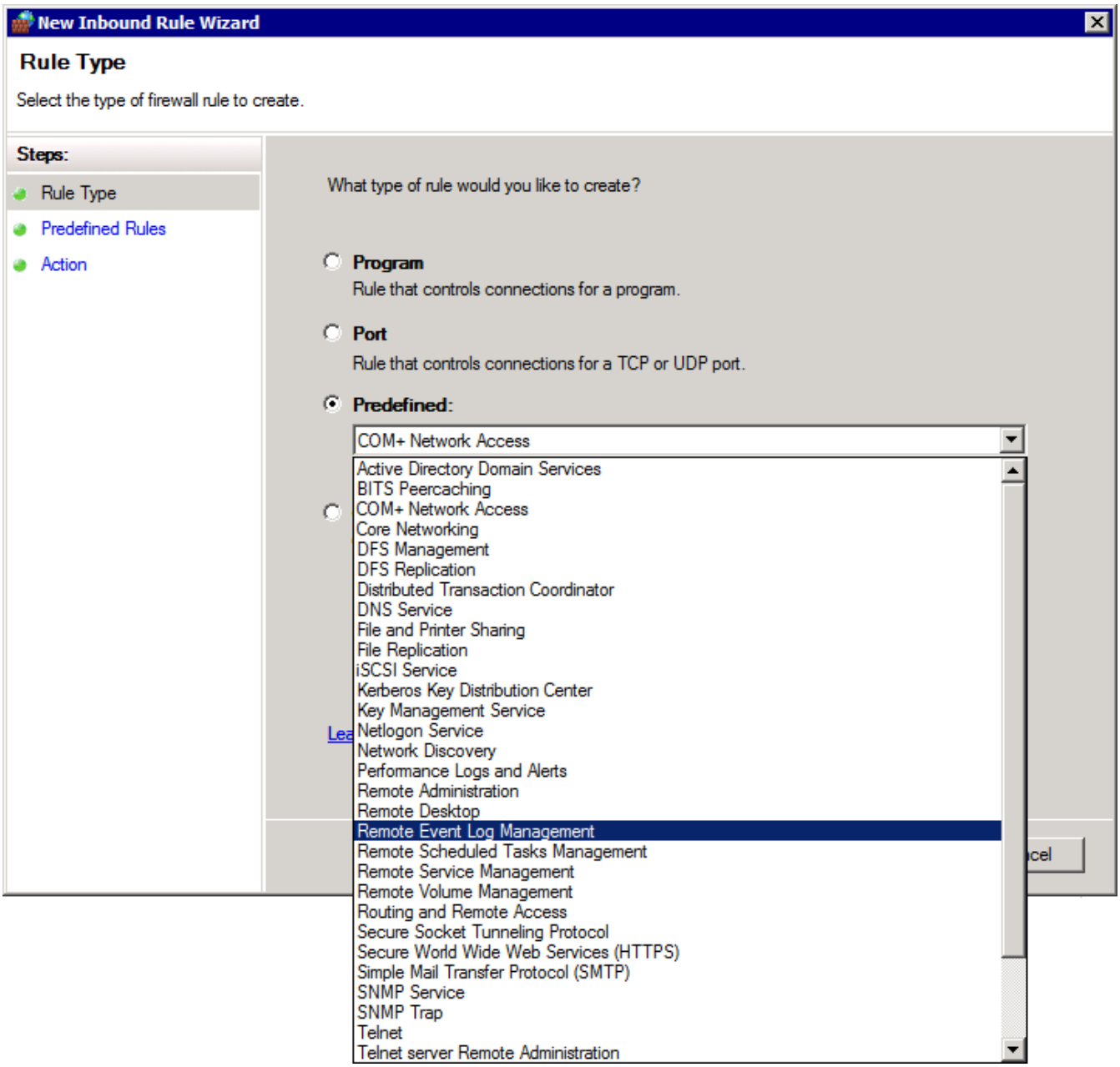
3. Right-click **Default Domain Policy** and select **Edit**.

4. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security**, right-click **Inbound Rules** and select **New Rule…**



Screenshot 287: Group Policy Management Editor

5. In the **New Inbound Rule** Wizard, select **Predefined** and select **File and Printer Sharing**.



Screenshot 288: Predefined rules

6. Click **Next**.

7. Select all rules and click **Next**.

8. Select **Allow the connection** and click **Finish**.

9. Repeat steps 5 to 8 for each of the following rules:

- Remote Event Log Management
- Network discovery.

10. From **Group Policy Management Editor**, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security**, right click **Outbound Rules** and select **New Rule…**

11. Repeat Steps 5 to 9 while at step 9 enable only **Network Discovery**.

12. Close **Group Policy Management Editor**.

13. From **Group Policy Management**, expand **Group Policy Management > Forest > Domains > <*Domain name*> > Default Domain Controllers Policy**.

14. Repeat steps 4 to 13.

15. Click **File > Save** to save the management console. The group policy comes into effect the next time each machine is restarted.

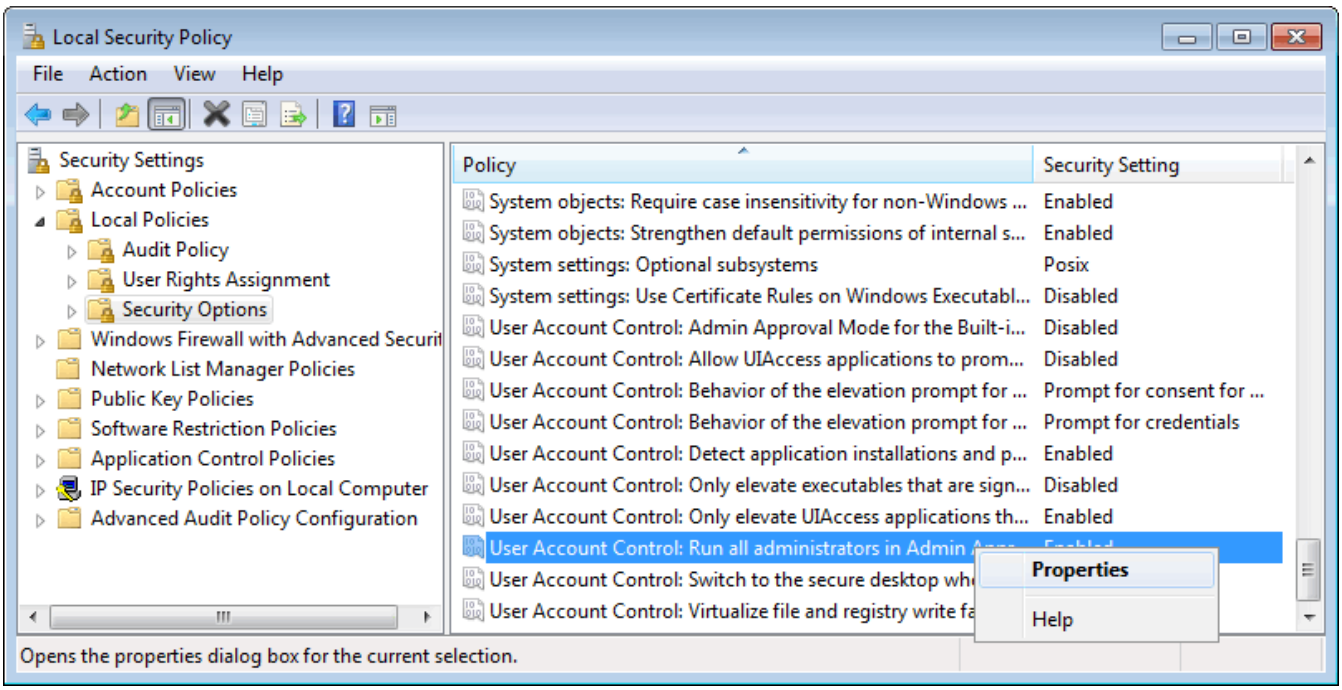
17.3 Disabling User Account Control (UAC)

When GFI EventsManager is configured to collect events using a local account target machines must have **User Account Control (UAC)** disabled. To disable UAC on Microsoft® Windows® Vista machines or later:

1. Click **Start > Run**, key in **secpol.msc** and press **Enter**.

2. From **Security Settings**, expand **Local Policies** and click **Security Options**.

3. Right-click **User Account Control: Run all administrators in Admin Approval Mode** and select **Properties**.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Securit
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy
Security Setting
System objects: Require case insensitivity for non-Windows ... Enabled
System objects: Strengthen default permissions of internal s... Enabled
System settings: Optional subsystems Posix
System settings: Use Certificate Rules on Windows Executabl... Disabled
User Account Control: Admin Approval Mode for the Built-i... Disabled
User Account Control: Allow UIAccess applications to prom... Disabled
User Account Control: Behavior of the elevation prompt for ... Prompt for consent for ...
User Account Control: Behavior of the elevation prompt for ... Prompt for credentials
User Account Control: Detect application installations and p... Enabled
User Account Control: Only elevate executables that are sign... Disabled
User Account Control: Only elevate UIAccess applications th... Enabled
User Account Control: Run all administrators in Admin
User Account Control: Switch to the secure desktop wh
User Account Control: Virtualize file and registry write fa
Properties
Help
Opens the properties dialog box for the current selection.

Screenshot 289: Disabling UAC

4. From the **Local Security Settings** tab, select **Enabled** and click **OK**.

5. Close the Local Security Policy window.

18 Troubleshooting

Use the information in the following sections to resolve issues encountered in GFI EventsManager:

- Documentation
- GFI SkyNet
- Request technical support
- Web forum
- Troubleshooter wizard

18.1 Documentation

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on: documentation@gfi.com.

18.2 GFI SkyNet

GFI maintains a comprehensive knowledge base repository, which includes answers to the most common problems. GFI SkyNet always has the most up-to-date listing of technical support questions and patches. In case the information in this guide does not solve your problems, next refer to GFI SkyNet by visiting: http://kb.gfi.com/.

18.3 Request technical support

If none of the resources listed above enable you to solve your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online**: Fill out the support request form and follow the instructions on this page closely to submit your support request on: http://support.gfi.com/supportrequestform.asp
- **Phone**: To obtain the correct technical support phone number for your region visit: http://www.gfi.com/company/contact.htm

> **Note**
>
> Before contacting Technical Support, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when first registering your license keys in the GFI Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

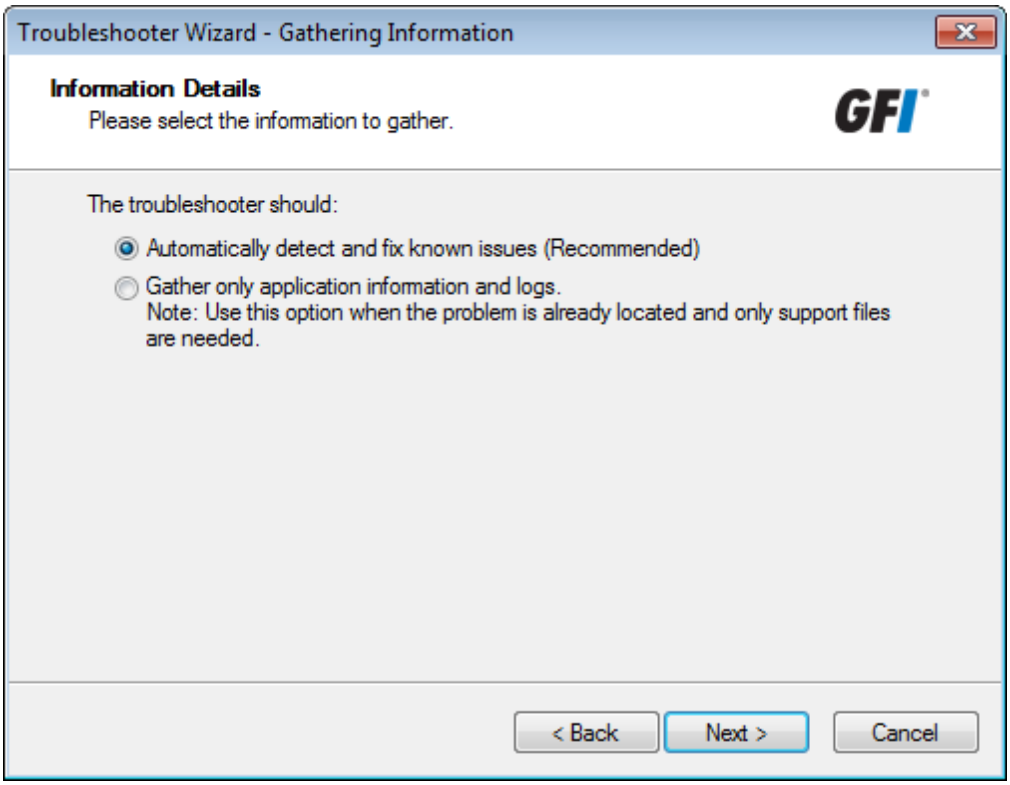
18.4 Web forum

User to user technical support is available via the GFI web forum. Access the web forum by visiting: http://forums.gfi.com

18.5 Troubleshooter wizard

To use the troubleshooting tool:

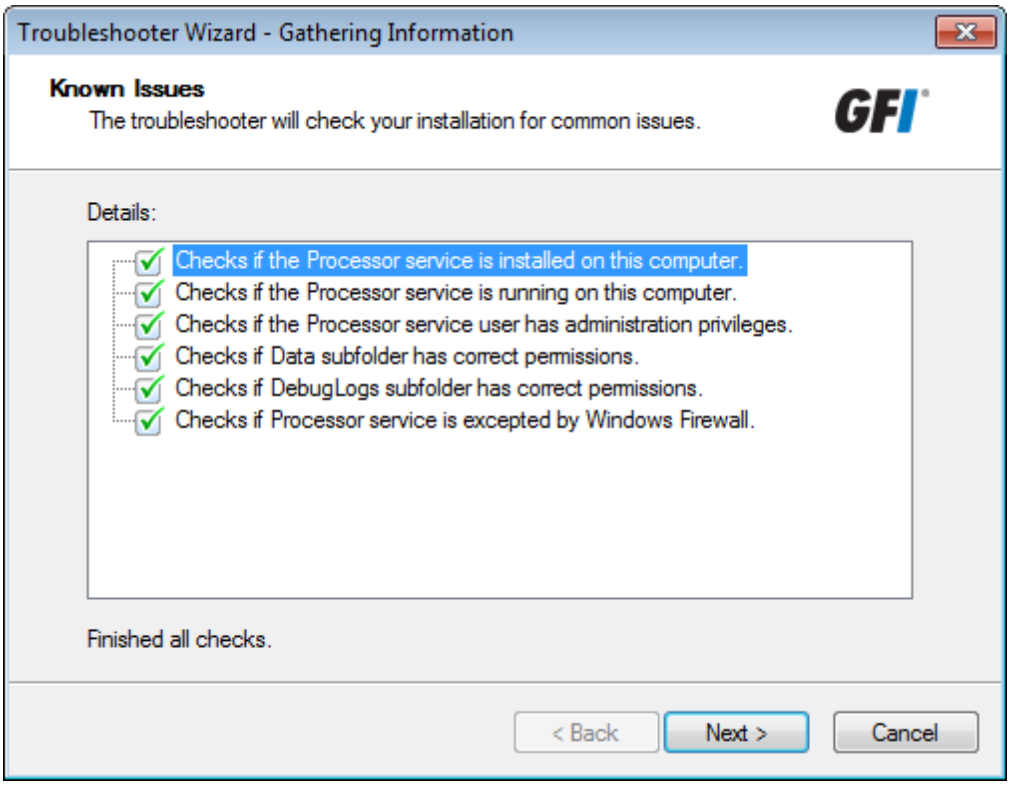
1. Go to the install folder of GFI EventsManager.
2. Locate and double-click **Trouble.exe**.
3. Click **Next** at the wizard welcome screen.


Troubleshooter Wizard - Gathering Information
Information Details
Please select the information to gather.
GFI
The troubleshooter should:
Automatically detect and fix known issues (Recommended)
Gather only application information and logs.
Note: Use this option when the problem is already located and only support files are needed.
< Back
Next >
Cancel

Screenshot 290: Select information gathering mode

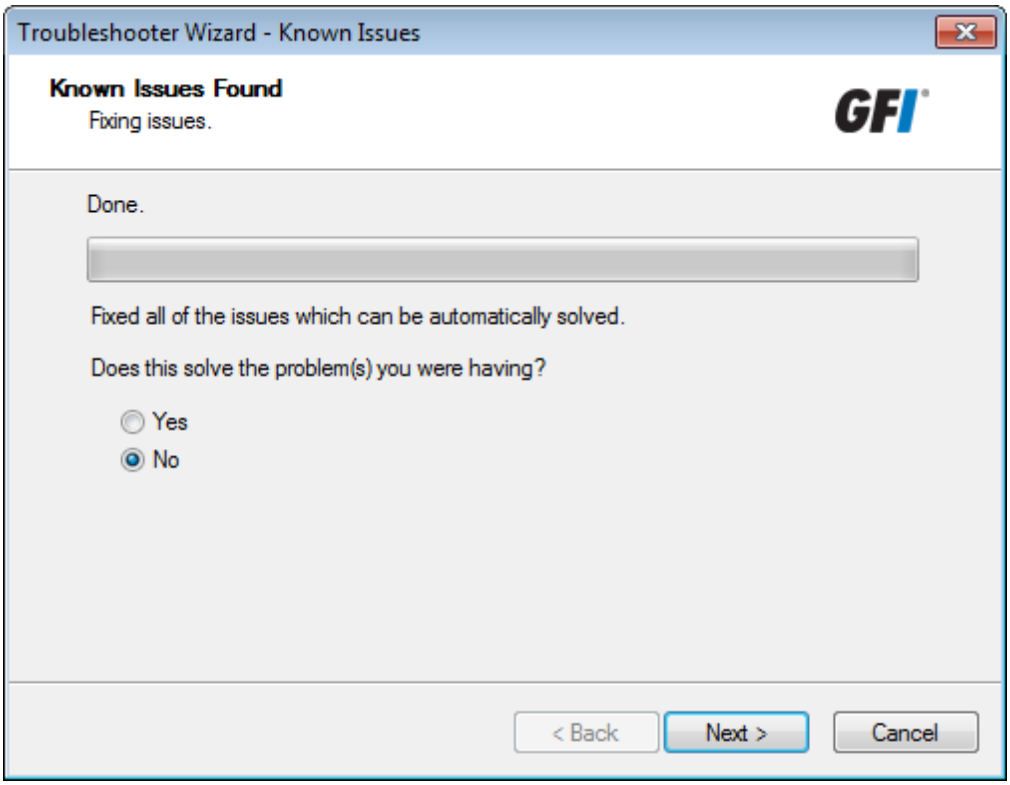
4. Select how the troubleshooter will collect information. Select from:

- **Automatically detect and fix known issues** - Select this option to allow GFI EventsManager to run a set of checks to determine what is wrong
- **Gather only application information and logs** - Specify your contact details, issue description and your system information to upload them to our support team. If you choose this option, skip to step **9**.


Troubleshooter Wizard - Gathering Information
Known Issues
The troubleshooter will check your installation for common issues.
GFI
Details:
Checks if the Processor service is installed on this computer.
Checks if the Processor service is running on this computer.
Checks if the Processor service user has administration privileges.
Checks if Data subfolder has correct permissions.
Checks if DebugLogs subfolder has correct permissions.
Checks if Processor service is excepted by Windows Firewall.
Finished all checks.
< Back
Next >
Cancel

Screenshot 291: Troubleshooter automatic checks

5. Wait for the troubleshooter to run the required checks and click **Next**.



Screenshot 292: Troubleshooter automatically fixing detected issues

6. Wait for the troubleshooter to apply fixes for issues detected during the check. If this solves your problem, click **Yes** and **Finish**. If the problem remains, select **No** and click **Next**.

Troubleshooter Wizard - Gathering Information
Search GFI Knowledge Base
Please fill in the appropriate information.
GFI
Enter search terms:
Cannot scan SQL Server sources
Search
Note: The search terms must be accurate. Entering more search terms will narrow your search and yield less results.
Search will be performed using the knowledge databases available at http://forums.gfi.com/ and http://kbase.gfi.com/.
Did the information found in the knowledge databases help you fix the issue(s)?
Yes
No
< Back
Next >
Cancel

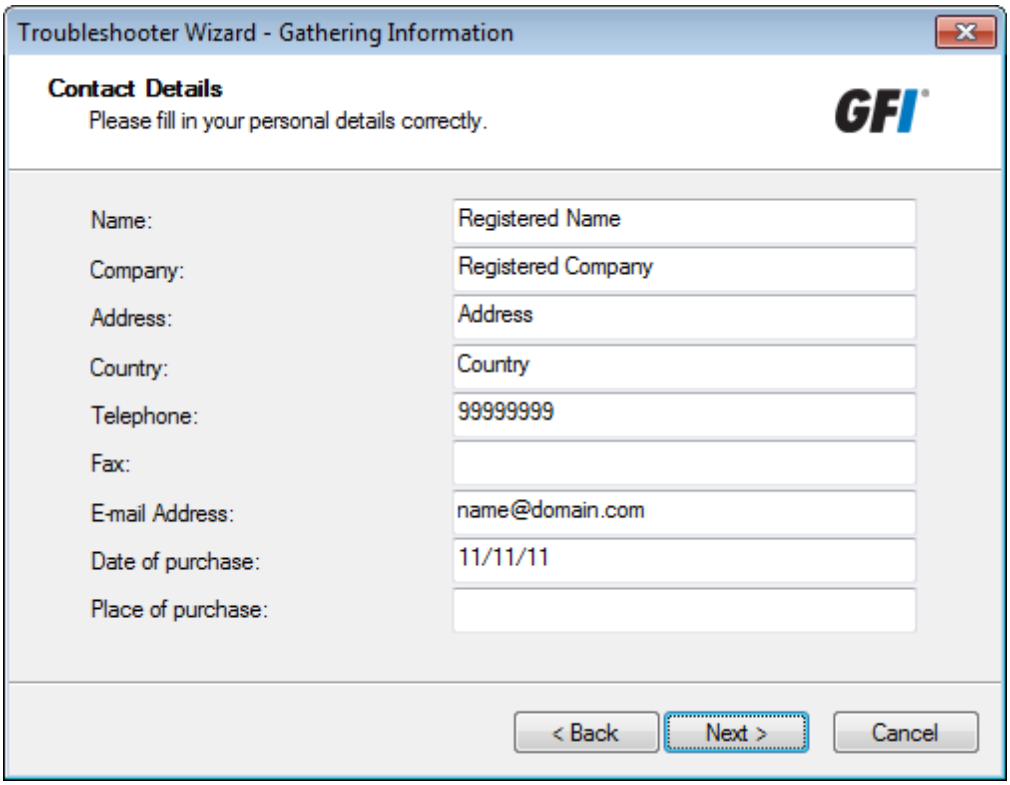
Screenshot 293: If the problem persists, search for articles on our knowledge base

7. Search our knowledge base archive for articles related to your problem. Key in the error your are encountering in the **Enter search items** text box and click **Search**. If this solves your problem, click **Yes** and **Finish**. If the problem remains, select **No** and click **Next**.

Troubleshooter Wizard - Gathering Information
More Information
The troubleshooter will collect further information.
GFI
The troubleshooter was unable to automatically locate your issue.
Next it will guide you through a wizard which will collect the information required by our support department in order to fix your issue(s).
< Back
Next >
Cancel

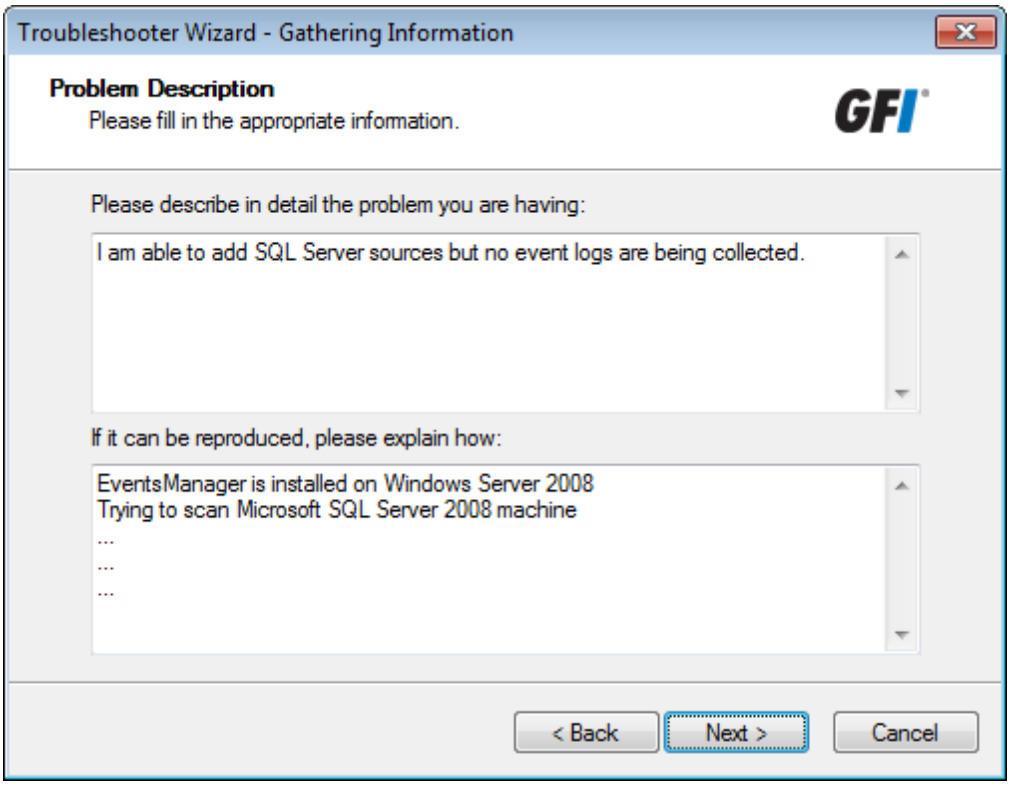
Screenshot 294: Manually checking for issues

8. Click **Next**.



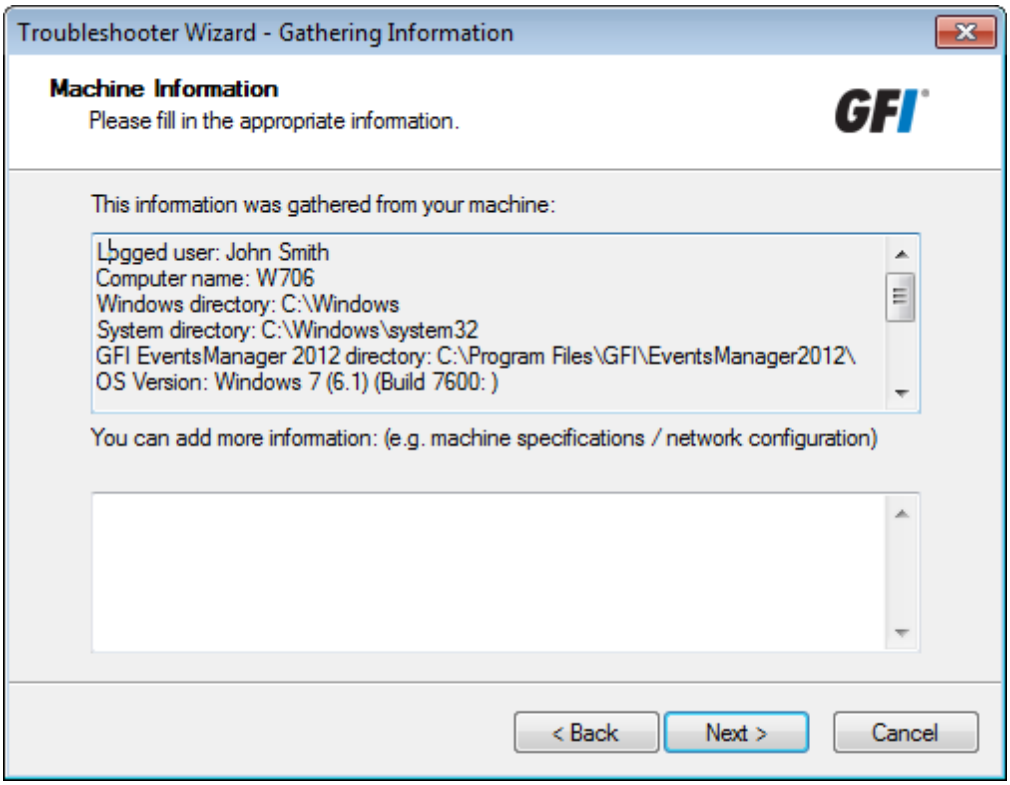
Screenshot 295: Specify contact details

9. Key in your contact details so that our support team would be able to contact you for further analysis information. Click **Next**.


Troubleshooter Wizard - Gathering Information
Problem Description
Please fill in the appropriate information.
GFI
Please describe in detail the problem you are having:
I am able to add SQL Server sources but no event logs are being collected.
If it can be reproduced, please explain how:
EventsManager is installed on Windows Server 2008
Trying to scan Microsoft SQL Server 2008 machine
...
...
...
< Back
Next >
Cancel

Screenshot 296: Key in the problem description and other information

10. Specify the error you are getting and other information that would help our support team to recreate this issue. Click **Next**.


Troubleshooter Wizard - Gathering Information
Machine Information
Please fill in the appropriate information.
GFI
This information was gathered from your machine:
Logged user: John Smith
Computer name: W706
Windows directory: C:\Windows
System directory: C:\Windows\system32
GFI EventsManager 2012 directory: C:\Program Files\GFI\EventsManager2012\
OS Version: Windows 7 (6.1) (Build 7600:)
You can add more information: (e.g. machine specifications / network configuration)
< Back
Next >
Cancel

Screenshot 297: Gathering machine information

11. The troubleshooter scans your system to get hardware information. You can manually add more information in the space provided or click **Next**.

Troubleshooter Wizard - Results
Completing the GFI EventsManager 2012 Troubleshooter Wizard
The file shown below is a 'ZIP' archive containing all the files that where gathered by this Wizard.
C:\Program Files\GFI\EventsManager2012\2012_04_12_203
Select 'Go to GFI Support...' for instructions on how to contact the GFI support department.
If the resulting 'ZIP' archive is larger than 4 MB, please select 'FTP Upload Instructions...' for instructions on how to upload this file to our FTP site.
FTP Upload Instructions...
Open Containing Folder...
Go to GFI Support...
< Back
Finish
Cancel

Screenshot 298: Finalizing the troubleshooting process

12. At this stage, the troubleshooter creates a package with the information gathered from the previous steps. Next, send this package to our support team so they can analyze and troubleshoot your problem. Select from:

- **FTP Upload Instructions** - Opens an article to give you instructions on how you can upload the troubleshooter package to our FTP server
- **Open Containing Folder** - Opens the folder containing the troubleshooter package so that you can send it via email
- **Go to GFI Support** - Opens the support page of GFI website.

13. Click **Finish**.

19 Glossary

A

Actions

The activity that will be carried out as a result to events matching specific conditions. For example you can trigger actions whenever an event is classified as critical. Actions supported by GFI EventsManager include Email alerts, event archiving and execution of scripts.

Alerts

Notifications which inform recipients that a particular event has occurred. GFI EventsManager can generate Email alerts, SMS alerts and Network alerts.

Archive

A collection of events stored in the SQL Server based database backed of GFI EventsManager.

Audit account management

Generates events when account management operations are done such as create/delete a user account or group, enable/disable a user account and set/change a user password. For more information, refer to http://technet.microsoft.com/en-us/library/cc737542(WS.10).aspx

Audit process tracking

Generates events which track actions such as programs which are launched, closed, as well as other indirect object access information which contain important security information. For more information, refer to http://technet.microsoft.com/en-us/library/cc775520(WS.10).aspx

Audit system events

Generates events when important system events happen such as user restarts or shuts down the target computer or when an event occurs that affects the security log. For more information, refer to http://technet.microsoft.com/en-us/library/cc782518(WS.10).aspx

C

COM+ Network Access

Enable this firewall permission to allow client machines to access applications or services that resides on the server. This allows GFI EventsManager to access resource from all servers. For more information about this permission, refer to http://technet.microsoft.com/en-us/library/cc731967.aspx

E

Email alerts

Email notifications which inform recipients that a particular event has occurred. To enable email alerts, you must have access to an active mail server.

Event classification

The categorization of events as Critical, High Medium, Low or Noise.

Event logs

A collection of entries which describe events that occurred on the network or on a computer system. GFI EventsManager supports different types of event logs including: Windows Event Log, W3C Logs, Syslog, SNMP Traps and SQL Server audit events.

Event processing rules

A set of instructions which are applied against an event log.

F

File and Printer sharing

Enable this firewall permission to allow GFI EventsManager to access events definitions on target machines. For more information, refer to http://technet.microsoft.com/en-us/library/cc779133(WS.10).aspx

I

Internet Protocol Security

A framework of open standards used to encrypt and authenticate network packets during a communication session between computers. Using cryptography services, IPsec ensures data integrity, authentication and confidentiality.

IPsec

Internet Protocol Security is a framework for a set of protocols for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the Application layer of the communications model. IPsec is said to be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

M

Management Information Base

A MIB is the equivalent of a data dictionary or codebook. It associates object identifiers (OIDs) with a readable label and various other parameters related to an active network object such as a router. Its main function is to assemble and interpret SNMP messages transmitted from SNMP-enabled network devices. The information stored in MIBs is organized hierarchically and is normally accessible using a protocol such as SNMP.

N

Network alerts

Network messages (known as Netsend messages) which inform recipients that a particular event has occurred. These messages are sent through an instant messenger system/protocol and are shown as a popup in the system tray of the recipient's desktop. To setup network alerts, you must specify the name or IP of the computers where the Netsend messages will be sent.

Network discovery

Enable this firewall permission to allow GFI EventsManager to gather information about connected machines on the network that can be scanned. For more information, refer to http://technet.microsoft.com/en-us/library/cc181373.aspx

Noise

Repeated log entries which report the same event.

O

Object auditing

Enable this auditing feature to audit events of users accessing objects (example, files, folder and printer). For more information, refer to http://technet.microsoft.com/en-us/library/cc976403.aspx

R

Remote Event Log Management

Required to allow GFI EventsManager to access and collect events from remote machines. For more information, refer to http://technet.microsoft.com/en-us/library/cc766438.aspx

Rule-set folder

The folder which contains one or more rule-sets.

Rule-sets

A collection of event processing rules.

S

SMS alerts

SMS notifications which inform recipients that a particular event has occurred. In GFI EventsManager, SMS alerts can be sent through various sources including mobile phones with modem capabilities and email-to-SMS web-based gateways.

SNMP Object Identifier (OID)

An SNMP object identifier is an address made up of a sequence of 'dotted' numbers (Example: 1.3.6.1.4.1.2682.1). These numbers uniquely identify and locate a specific device (Example: hub) within the entire network. SNMP OIDs are a key component in the assembly of SNMP messages. In fact, an SNMP server cannot interpret or assemble messages which don't have an OID. Individual vendors often create their own MIBs that only include the OIDs associated specifically with their device.

SNMP Traps

Notifications/alerts generated and transmitted by active network components (Example: hubs, routers and bridges) to SNMP server(s) whenever important events such as faults or security violations occur. Data contained in SNMP Traps may contain configuration, status as well as statistical information such as number of device failures to date.

Syslog messages

Notifications/alerts most commonly generated and transmitted to a Syslog server by UNIX and Linux-based systems whenever important events occur. Syslog messages can be generated by workstations, servers as well as active network devices and appliances such as Cisco routers and Cisco PIX firewalls to record failures and security violations amongst other activities.

U

Unclassified events

Events that did not satisfy any of the event processing conditions configured in the event processing rules.

W

W3C logs

W3C is a common log format developed by the World Wide Web Consortium. W3C logs are text-based flat files used mainly by web servers including Microsoft Internet Information Server (IIS) to record web related events such as web logs.

Windows Event Logs

A collection of entries which describe events that occurred on a computer system running Windows OS.

20 Index

A

Activity Monitoring 55, 63, 66, 134

Alerting Options 54, 63-64, 145, 210, 225, 232, 309

Alerts 24, 55, 63-64, 80, 136, 159, 173-174, 187, 208, 210, 216, 224, 287

Anonymization 62, 235, 246, 278, 311

Antivirus 32, 117

Archive 24, 32, 72, 80, 84, 94, 103, 105, 108, 112, 173, 183, 209, 343

Audit Options 98, 232-233, 238

Auto Update 287

B

Backup 138, 168, 215, 323

C

Checks 64, 72, 74, 78, 173, 177, 183, 190, 192, 196, 201, 206-207, 210, 212, 247, 341

Classification 64, 174, 181, 185, 208

Color Coding 124, 131

Console Security 62, 232, 236, 238, 240

Credentials 41, 50, 58, 60, 68, 72, 74, 82, 92, 235, 239, 263, 273, 288

CSV 72, 76, 105, 124, 165, 167, 322

Custom Event Logs 115

D

Daily Digest 158-159

Dashboard 55, 63, 134, 249

Database 22, 31, 38, 44, 55, 81-82, 89, 100, 117, 124, 126, 137, 164, 166, 176, 215, 242-243, 245, 250, 252, 259, 263, 271, 281, 283, 311, 318

Database Backend 33, 43, 52, 84, 94, 138, 242, 244, 302

Database Operations 54, 251, 253, 257, 261, 266, 269, 271, 275, 279, 282

Database Servers Groups 81, 90

Default Classification Actions 63, 182, 187, 192, 208, 295

Demilitarized Zone 27, 29

Deployment 26, 28-29

DLib 38, 47, 311

DLib Database Server 37, 44, 311

DMZ 29

DNS 27-28, 30, 35, 100

E

Email 63, 173, 176, 212

Email Alerts 183, 209-210, 218, 224

Event Finder 127

Event Source 24, 32, 54, 57, 59, 63-64, 67-68, 71, 73-74, 76-78, 80-81, 90, 101, 104, 107, 111, 117, 139, 161, 164, 166, 180, 185, 195, 200, 205-206, 210, 286, 293, 321, 326, 334

Event Sources 24, 32, 54-56, 60, 63-64, 67-68, 71, 73, 75, 77-78, 80-81, 90, 100-101, 104, 107, 111, 118, 126, 136, 161-163, 181, 190, 194, 197, 204, 206, 210, 228, 239, 250, 294-295, 310, 321, 326

Event Sources Groups 67-68, 71, 73, 75, 77, 79-80

Events Browser 22, 31, 63, 123-124, 127, 130, 132, 183, 192, 235, 242-243, 295

Events Processing Rules 24, 54-55, 63, 65-66, 80, 103, 105, 108, 112, 120, 122, 127, 173, 175, 178, 189-190, 195, 199, 302

EventsManagerAdministrator 216, 309

Export 31, 36, 124, 138, 142, 166, 168, 242, 252-253, 257, 261, 267, 270, 272, 276, 280

Export Data 31, 139-140, 165-166, 253, 260, 265, 269, 314

F

File Storage 31, 43, 52, 137, 242, 244, 246-247, 250, 253, 280, 310

Firewall 22, 29, 32, 62, 108, 114, 326-327, 330, 332-333, 335-336

G

General View 135

GFI EndPointSecurity 28, 65, 121, 165-166

GFI LanGuard 28, 116, 136, 165-166

Groups 35, 62, 67-68, 77, 81, 90, 136, 171, 216, 220, 222, 229, 234, 303

H

Hashing 242, 245

I

Import 36, 68, 86, 95, 126, 242, 253, 262, 267, 270-271, 275, 279

Installation 36, 44, 53, 127, 143, 301

J

Job Activity View 138

L

LAN 27-29, 247

License 37, 46, 71, 73, 76, 307, 340

Licensing 72, 76, 285, 293

Logon 41, 50, 60, 63, 68, 72-74, 82, 90, 100, 134, 143, 177, 180, 212, 263, 273, 288, 307

M

Monitor 22, 27-29, 34, 44, 62, 66, 81, 90, 116, 122, 232

N

Network Alerts 213

O

Operational History 56, 61, 139, 158, 164, 167

P

Performance Options 285

ports 121, 137

Protocols 33, 137, 176

Q

Quick Launch Console 53, 55

R

Reporting 55, 66, 124, 141-142, 144, 146, 152, 158, 169-170, 176, 303

Reports 65, 142-144, 146, 152, 158, 170, 237, 303

Root Folder 144, 152, 192, 196, 207

Rule-sets 175

Rule Folders 189, 303

S

SMS Alerts 210

SNMP 22, 24, 33, 63, 72, 76, 81, 110, 137, 139-140, 164, 166, 176, 183, 190, 210

Statistics View 139

Status 55, 61, 120, 122, 134, 138-139, 165-166, 237, 243, 249, 282, 293, 321

Syslog 24, 30, 34, 55, 60, 68, 72, 81, 137, 140, 143, 176, 214

Syslog Server Options 109

T

Text Logs 22, 24, 28, 72, 76, 80, 103, 110, 124, 136, 140, 176, 179, 212, 313

U

Users 62, 98, 116, 121, 137, 143, 145, 159, 171, 190, 209, 216, 222, 229, 232, 239, 287, 302

V

Version 294

W

WAN 27, 31

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104 Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.com

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

GFI®